
# REAL WORLD SERVERLESS

## Going Lambda without being burned too much

# DAVID SCHMITZ
# SENACOR TECHNOLOGIES
# @KOENIGHOTZE

# 4 QUESTIONS

# MICROSERVICES

MICROSERVICES

**CONTAINERS**

MICROSERVICES

CONTAINERS

**CLOUD**

MICROSERVICES

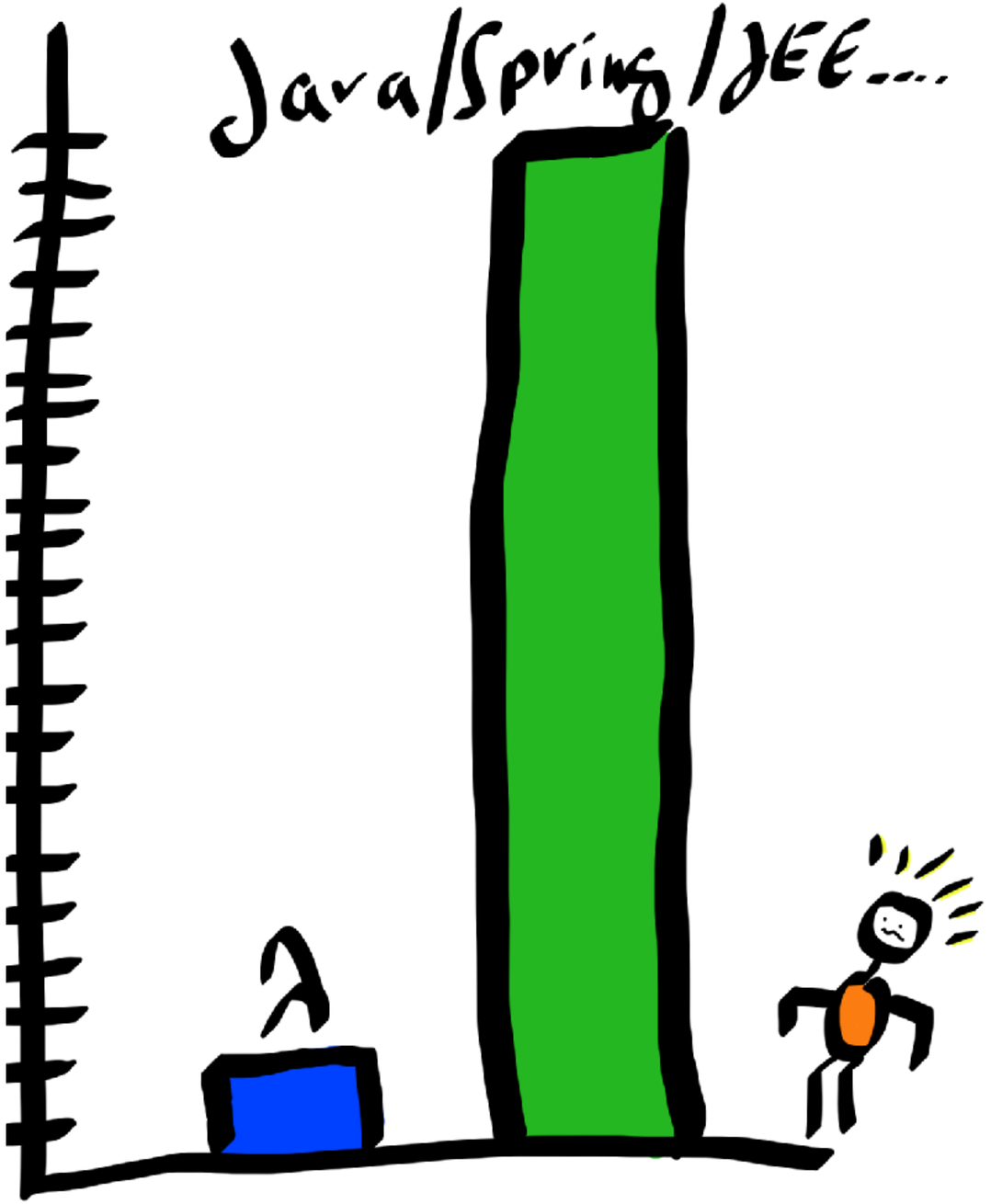
CONTAINERS

CLOUD

**SERVERLESS**


# VENDOR?

# CLOUD GURU?


Java/Spring/JEE....
λ

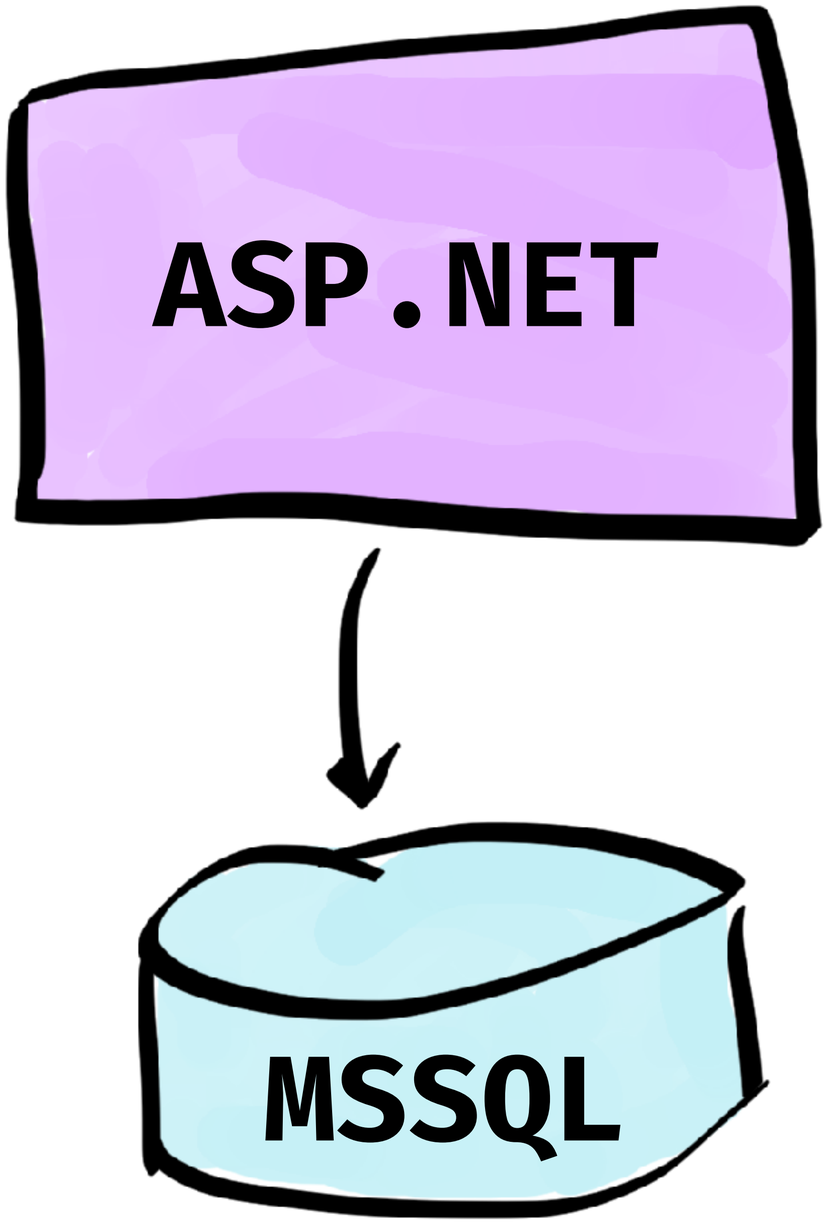
# THINGS ARE MOVING

# FAST

# EXPECTATION MANAGEMENT

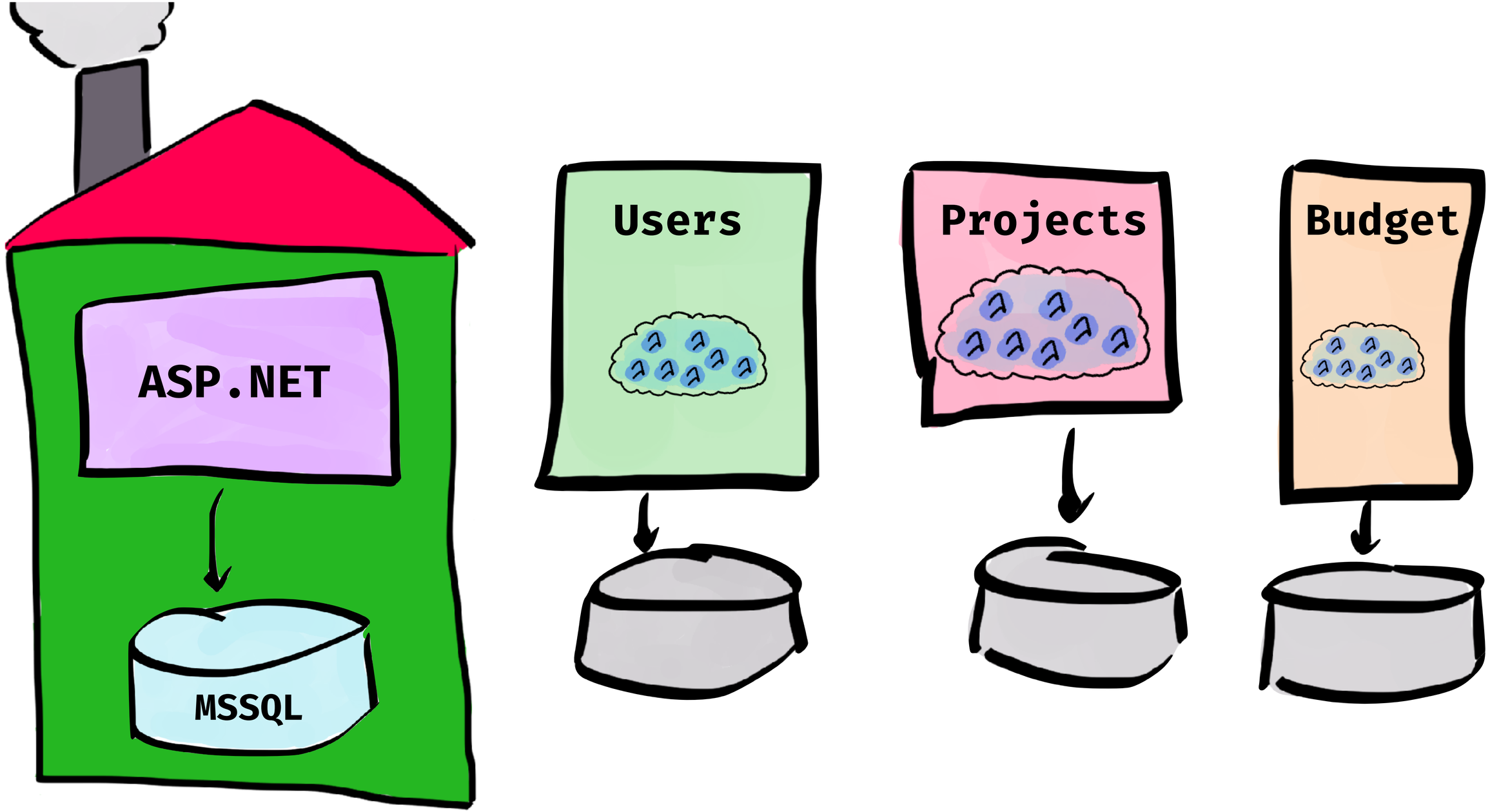
“Some of the things we learned, while moving an application (partially) to AWS Lambda.”

*–Me*




# EMPLOYEE ADMINISTRATION PLATFORM

# TARGET ARCHITECTURE


ASP.NET
MSSQL
Users
Projects
Budget

# WORK IN PROGRESS!

# Some basics

# Some basics

# Security

# Some basics

# Tools and stuff

# Security

Some basics

Architecture

Tools and stuff

Security

Some basics

Architecture

Tools and stuff

Housekeeping

Security

Some basics

Operations

Architecture

Tools and stuff

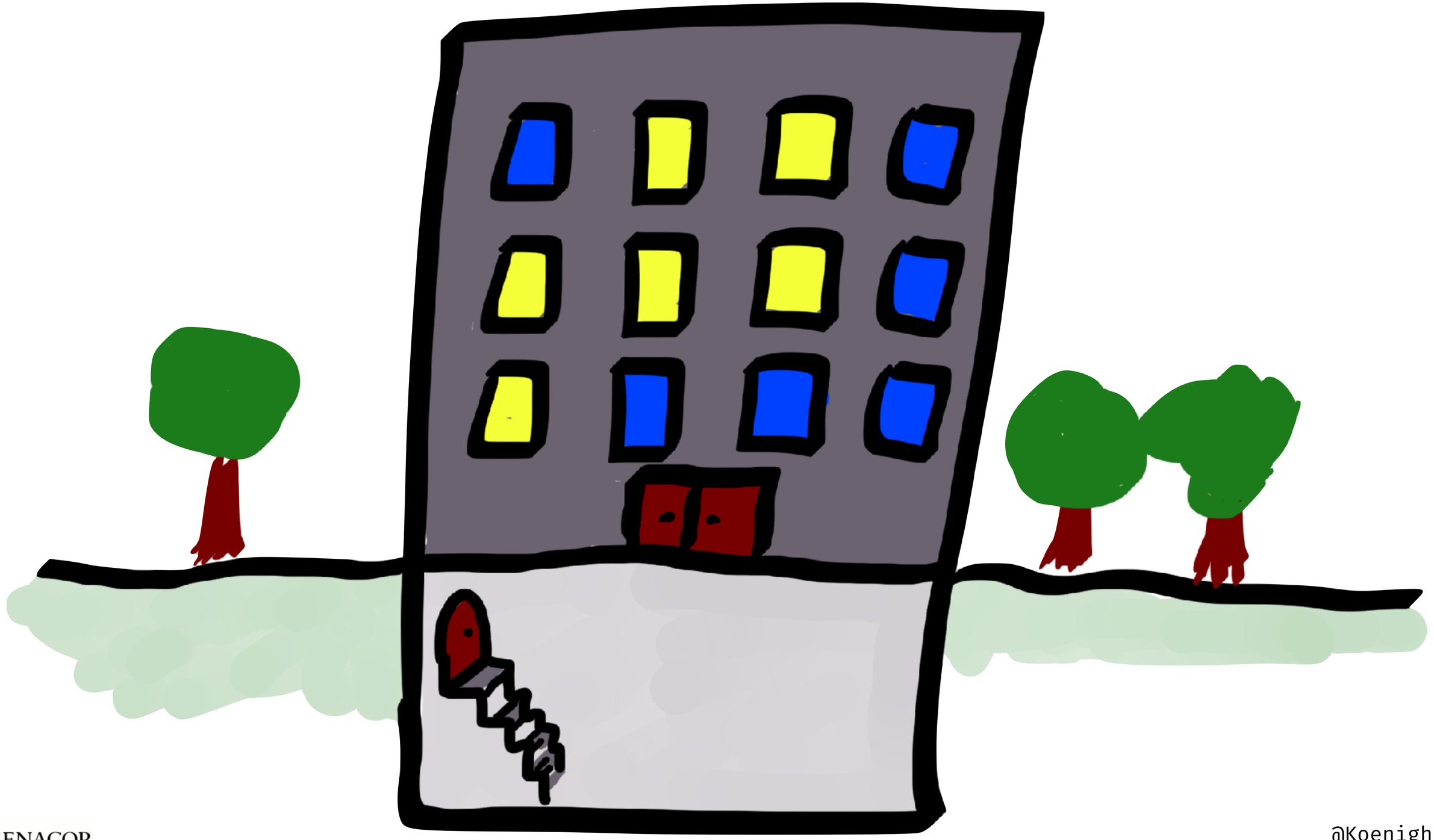
Housekeeping

Security


# AWS LAMBDA 1-0-1

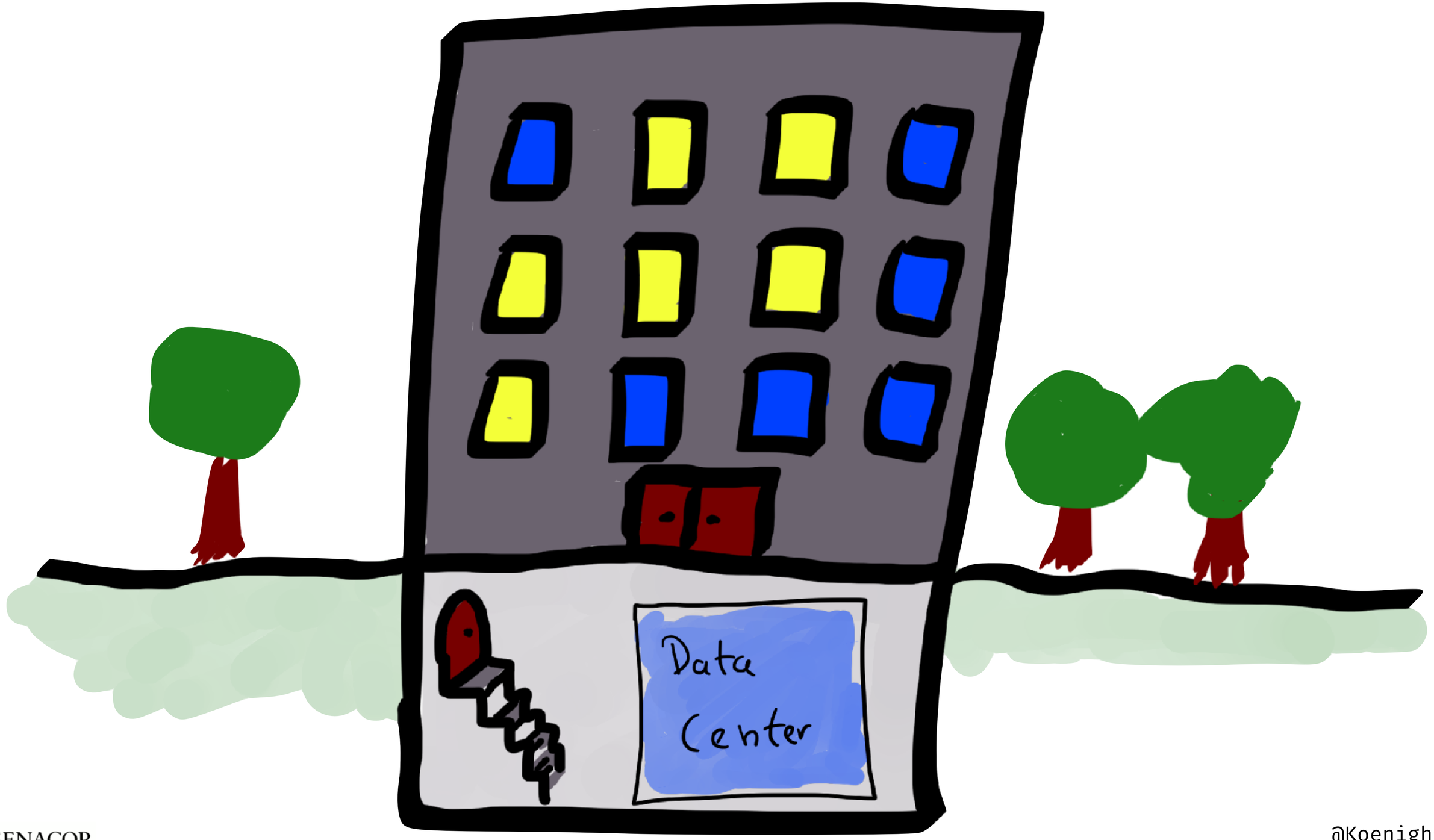
@Koenighotze

# *Ye olde days*



SENACOR

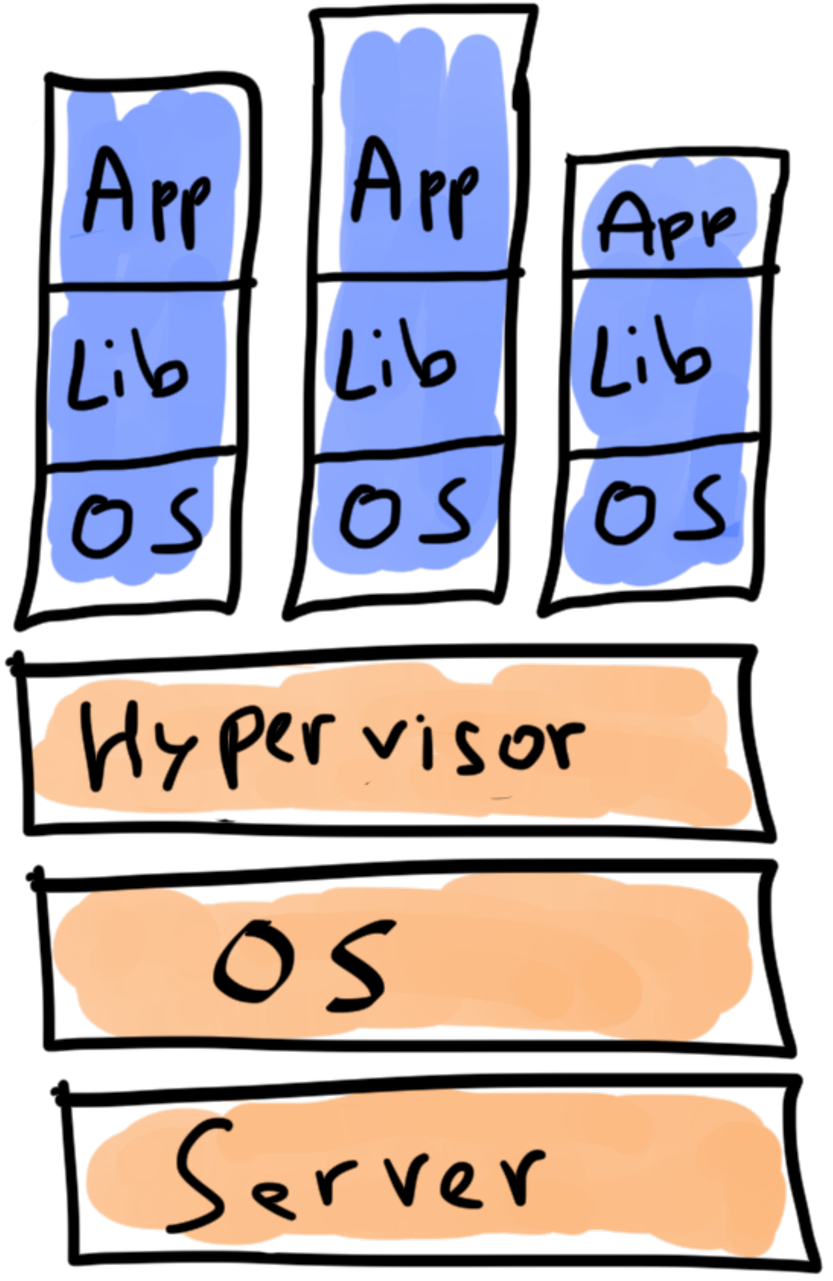
@Koenighotze



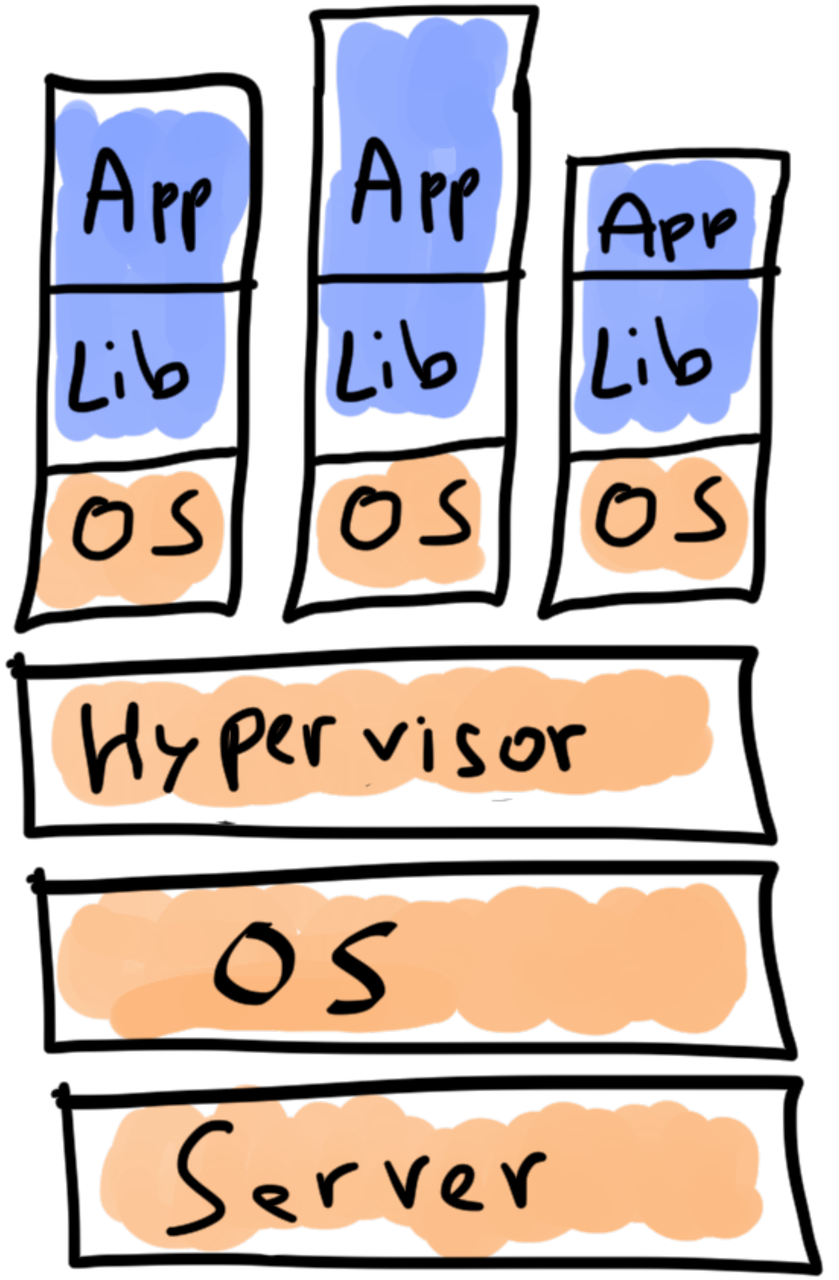

SENACOR

@Koenighotze

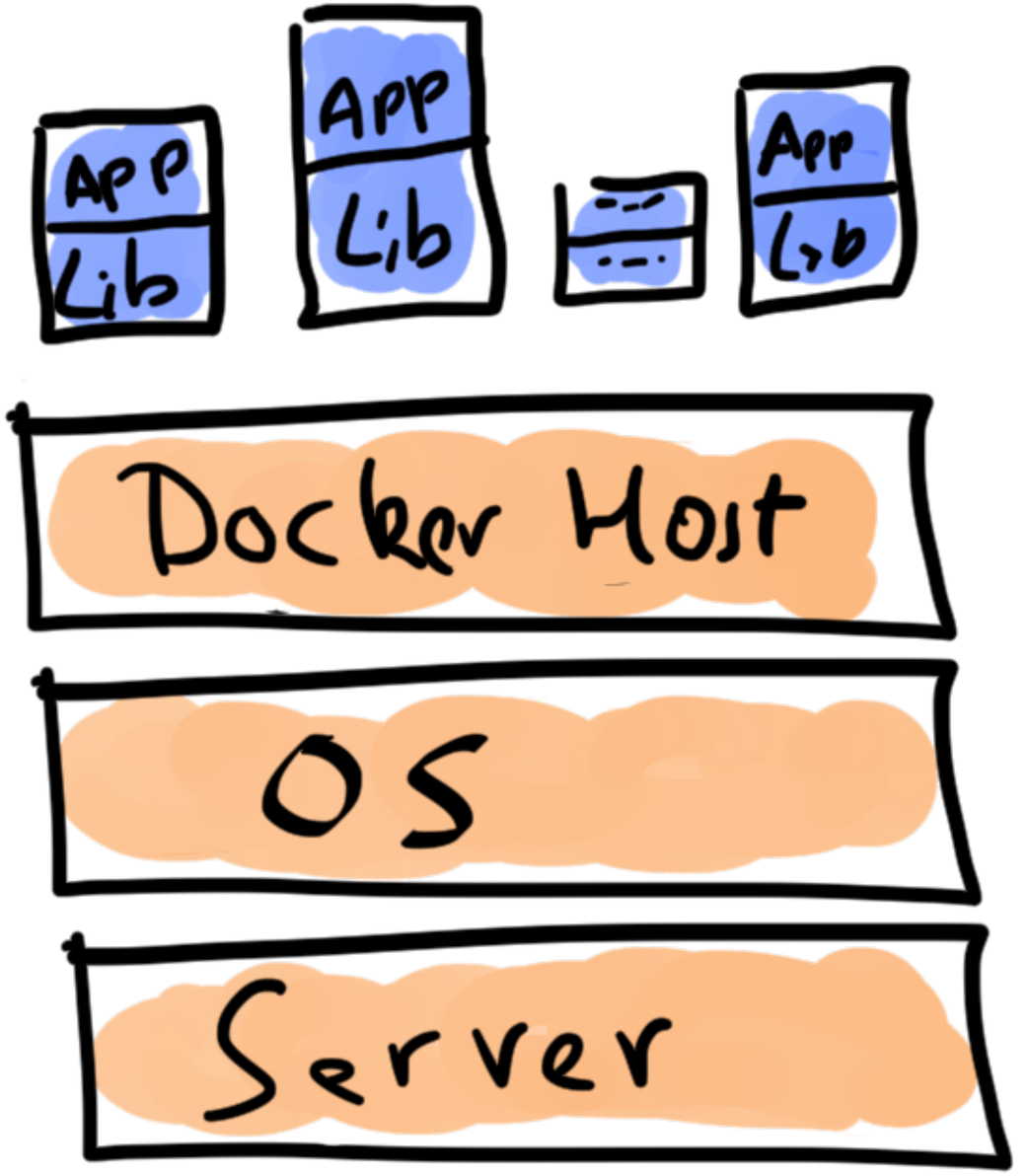
# INFRASTRUCTURE AS A SERVICE

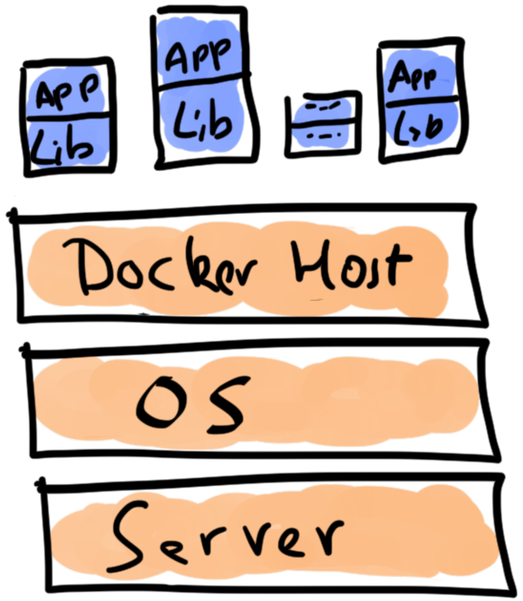

App
Lib
OS
App
Lib
OS
App
Lib
OS
Hypervisor
OS
Server

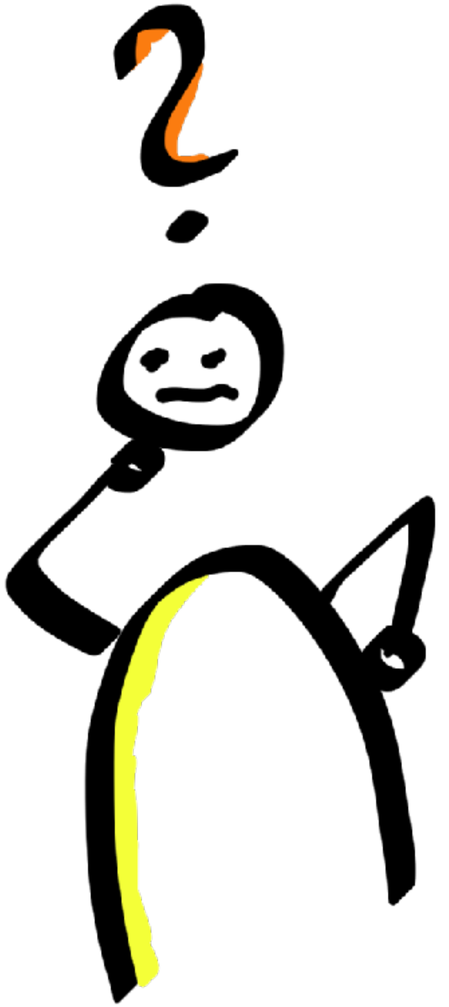
# PLATFORM AS A SERVICE


App
Lib
OS
App
Lib
OS
App
Lib
OS
Hypervisor
OS
Server

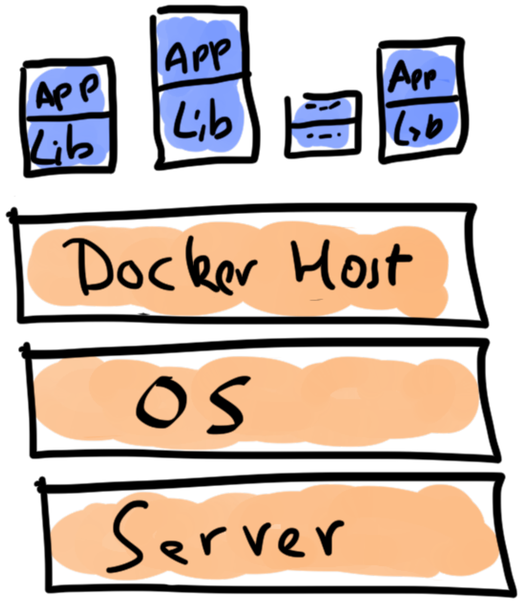
# CONTAINERS

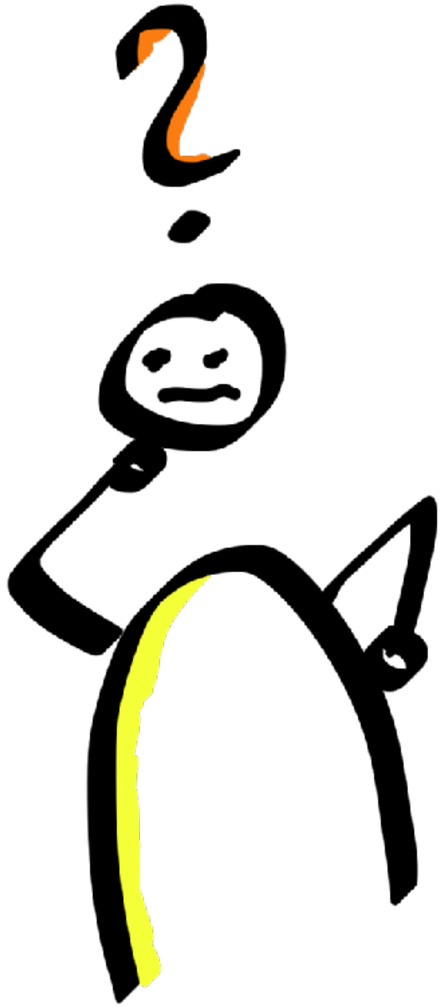

App
Lib
App
Lib
App
Lib
Docker Host
OS
Server


App
Lib
App
Lib
App
Lib
Docker Host
OS
Server



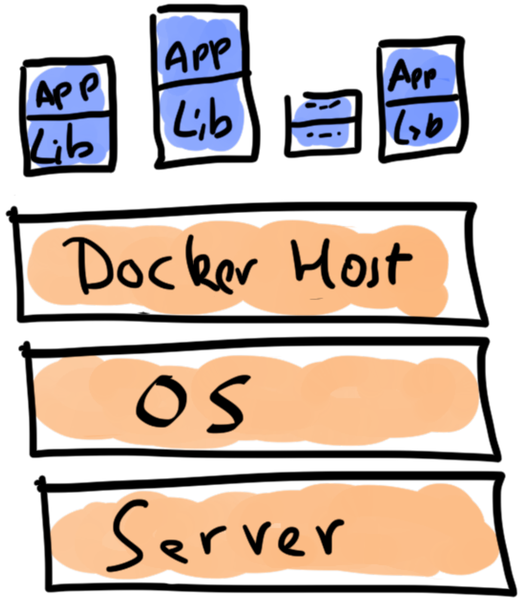
# Provisioning

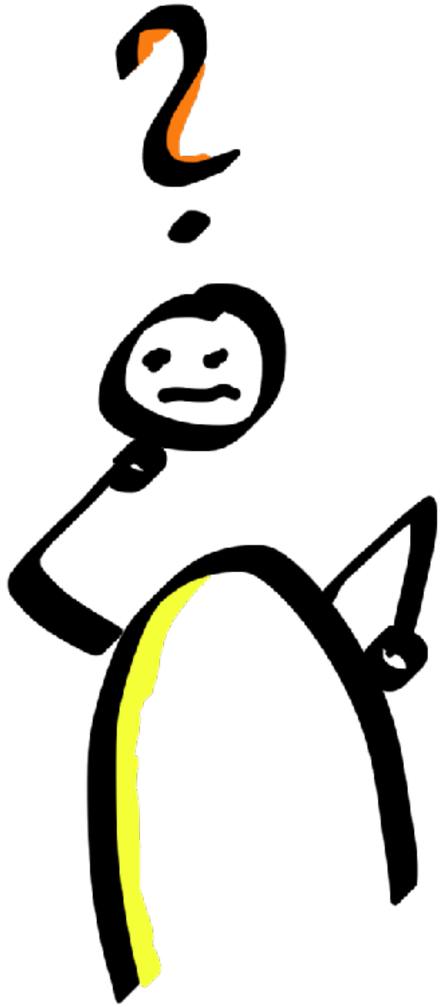


# Provisioning

# Scaling

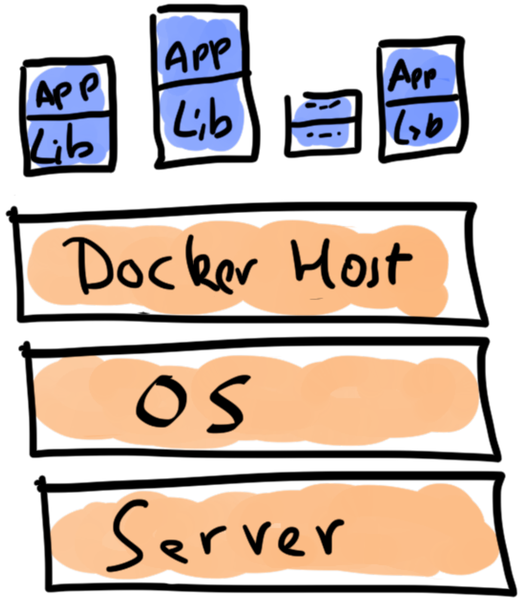


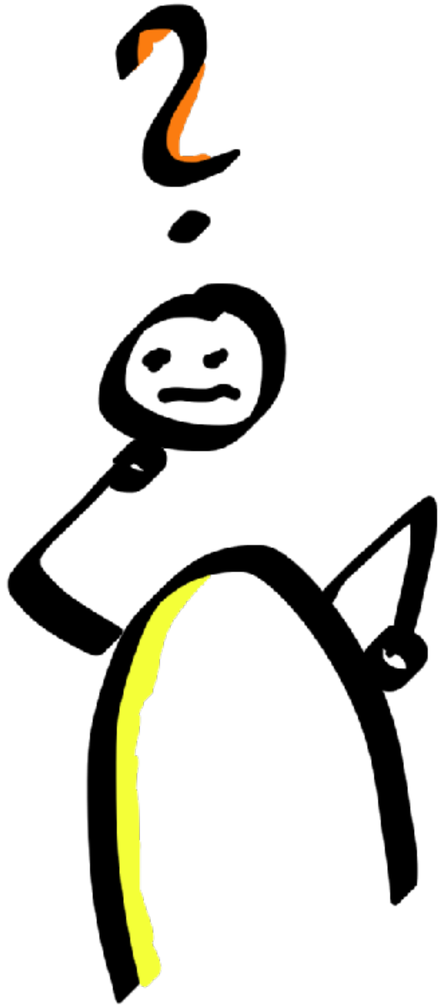



Provisioning

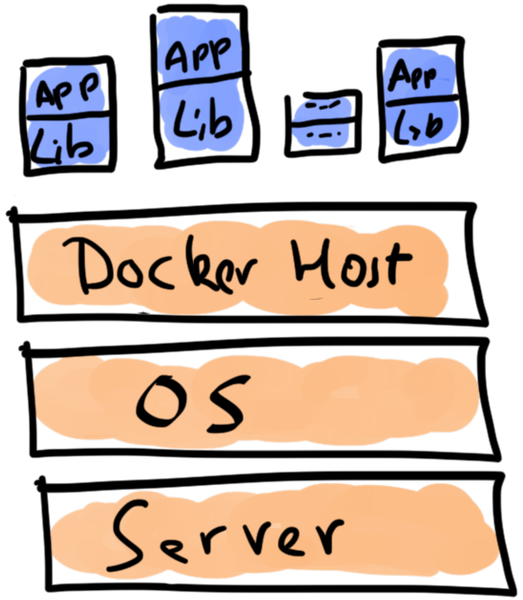
Scaling

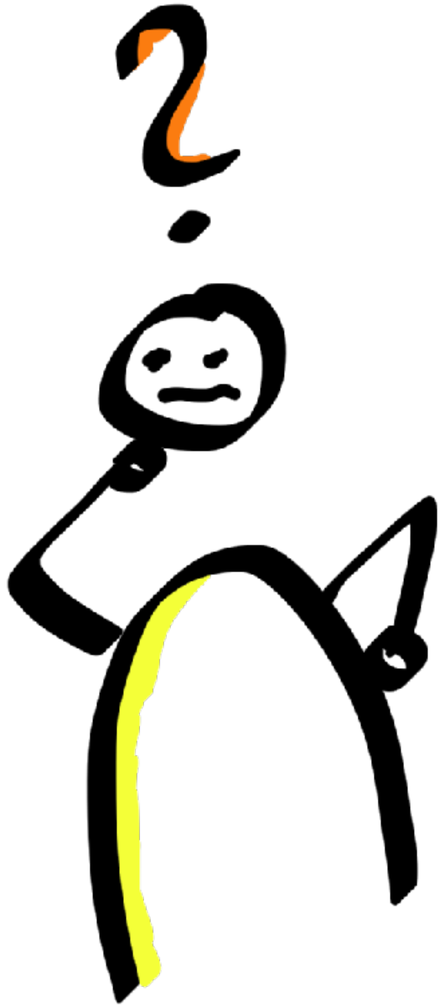
**Monitoring**



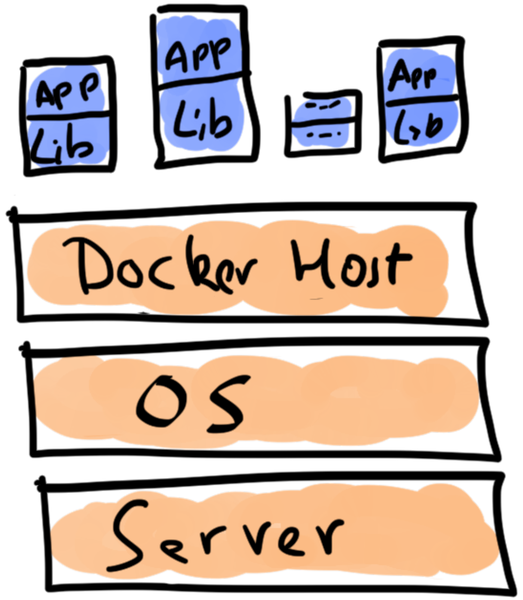



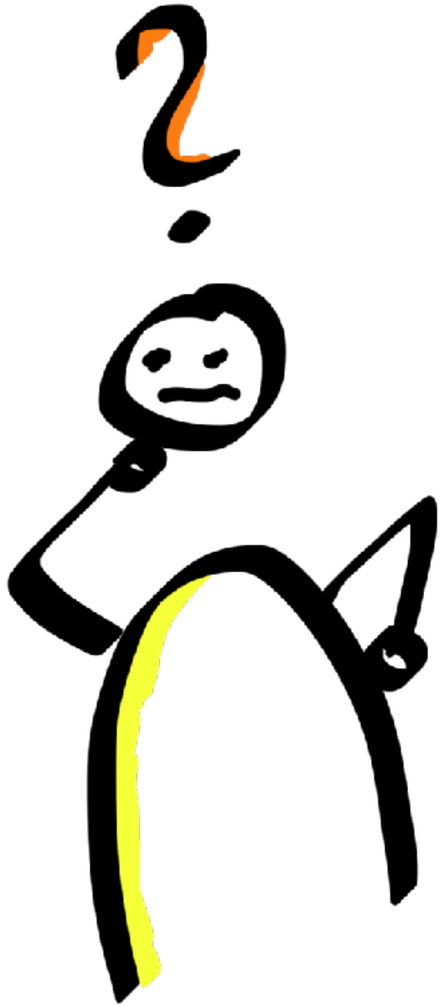
Provisioning
Scaling
Monitoring
**State**



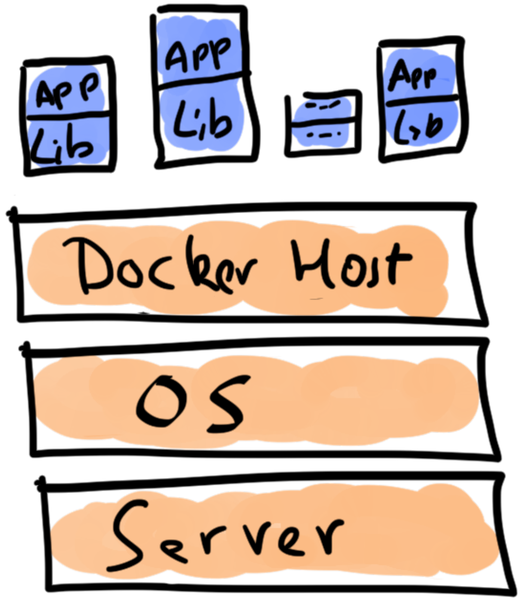



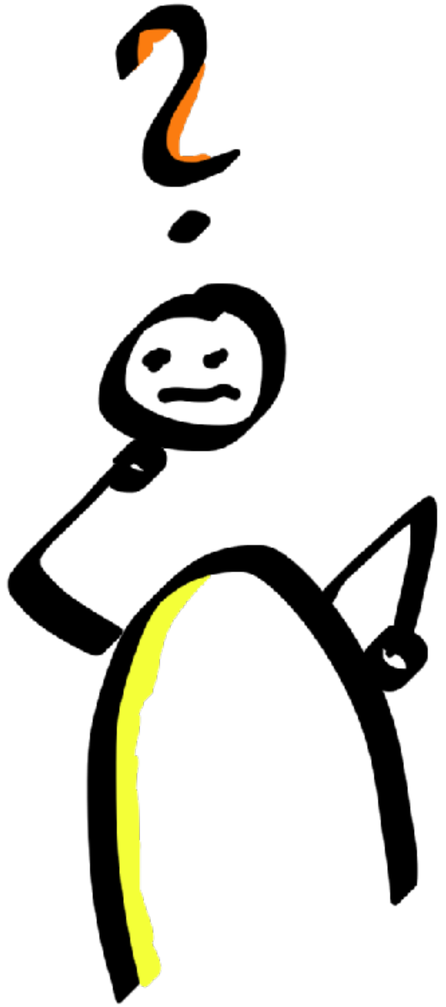
Provisioning
Scaling
Monitoring
State
**Security**



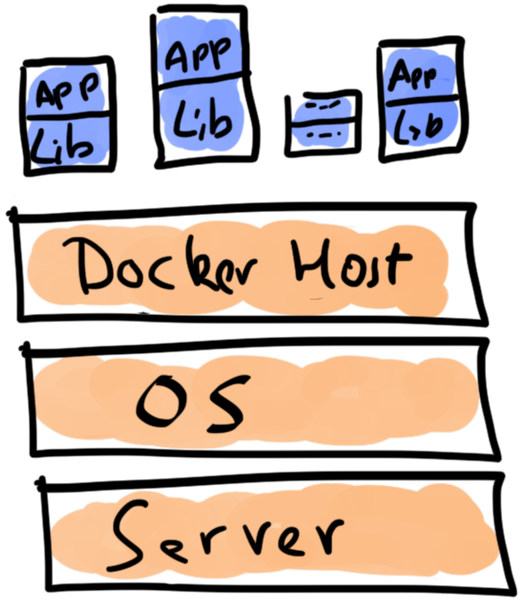



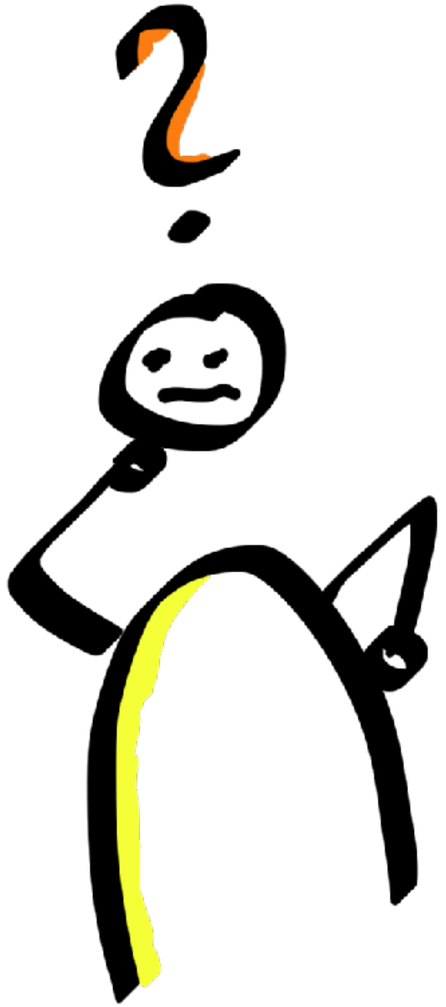
Provisioning
Scaling
Monitoring
State
Security
**Deploying**



# Provisioning
# Scaling
# Monitoring
# State
# Security
# Deploying

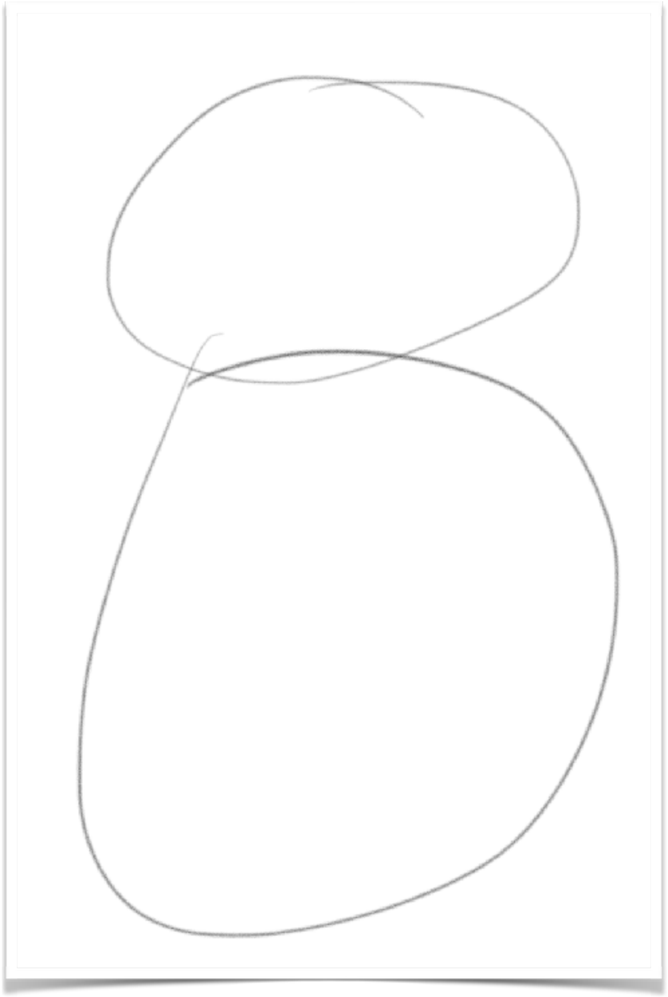


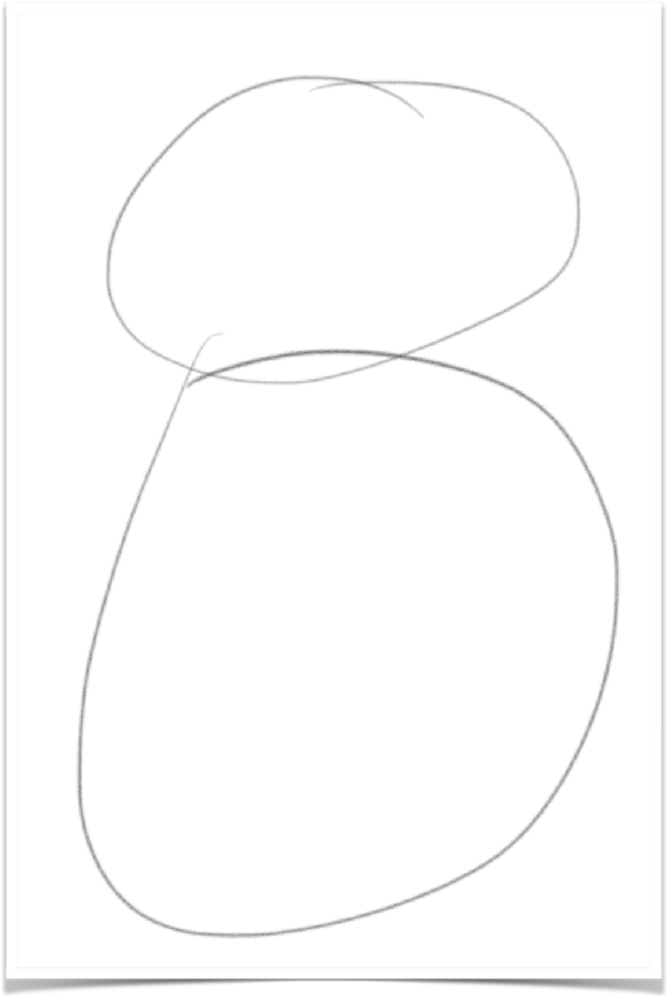
●●●

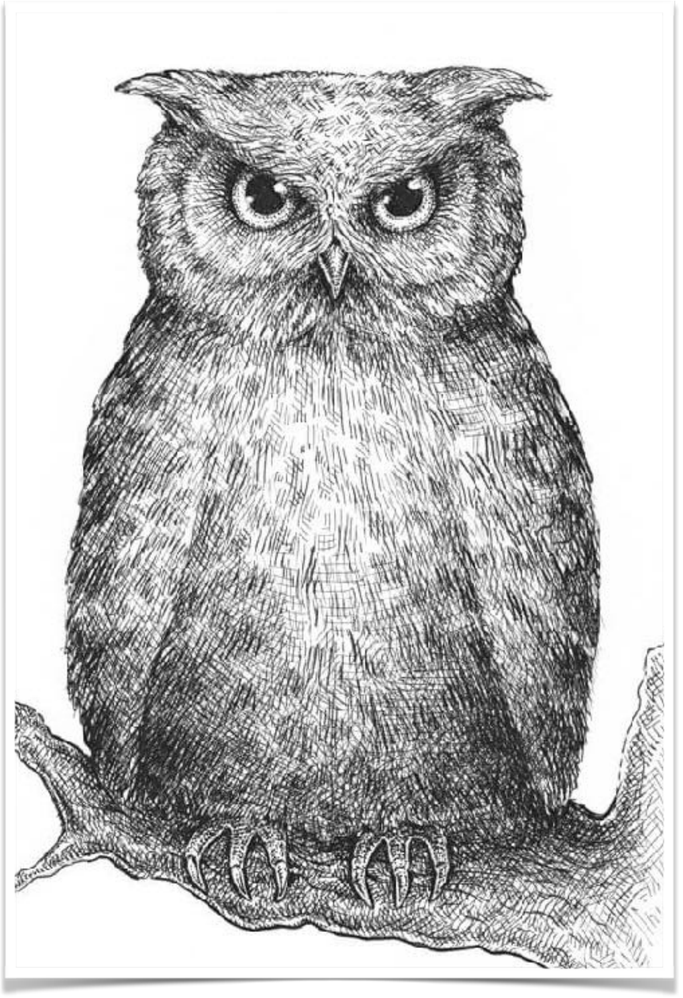
# DESIGNING DISTRIBUTED SYSTEMS IS DIFFICULT

# HOW TO DRAW AN OWL?



# 1. Draw some circles

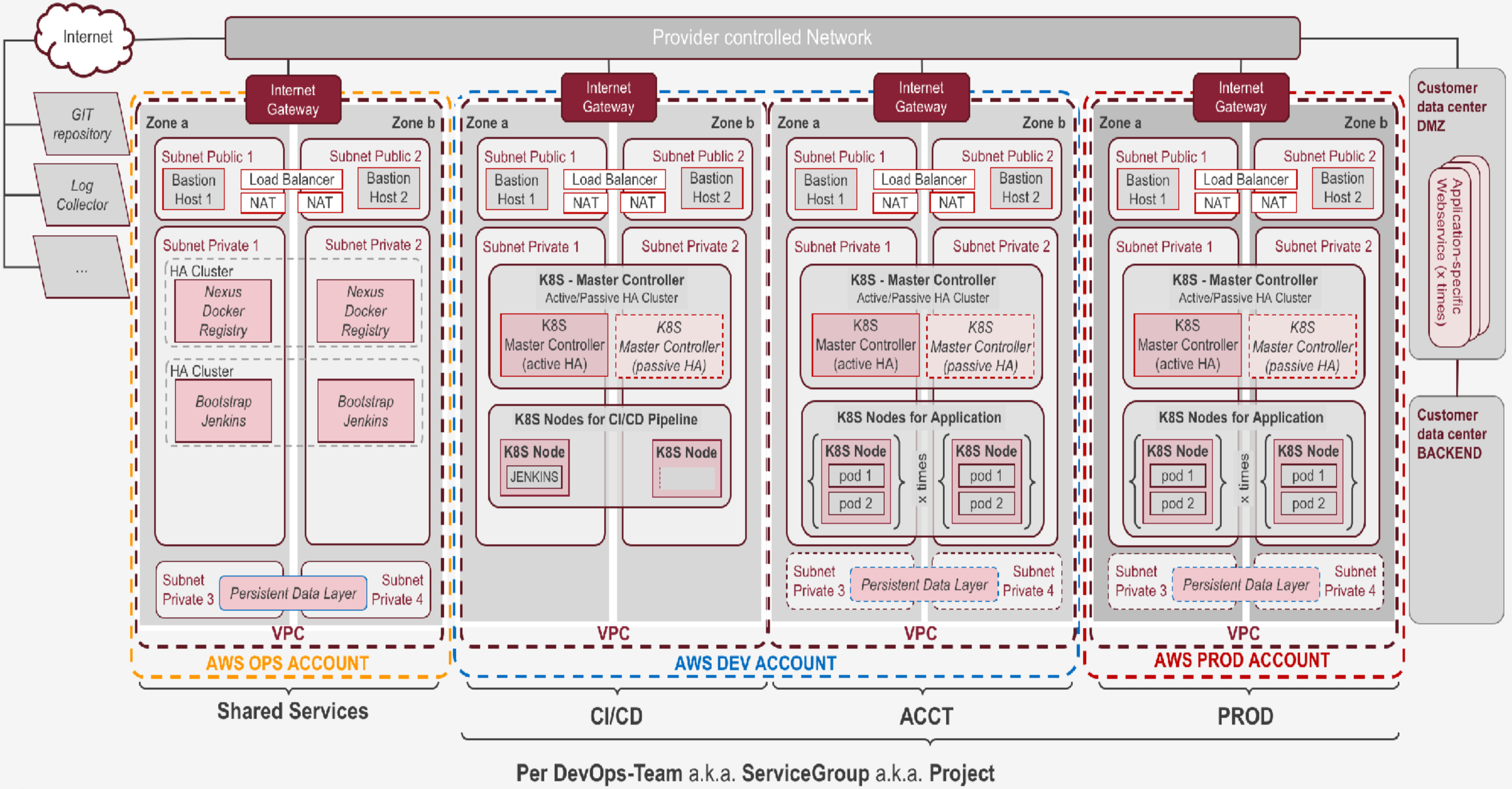




1. Draw some circles

2. Draw the rest of the damn owl

# kubernetes




SENACOR

@Koenighotze

# ENTER SERVERLESS

# SO WHAT IS SERVERLESS?

**Serverless computing allows you to build and run applications and services without thinking about servers. Serverless applications don't require you to provision, scale, and manage any servers…**

**Building serverless applications means that your developers can focus on their core product instead of worrying about managing and operating servers or runtimes…**

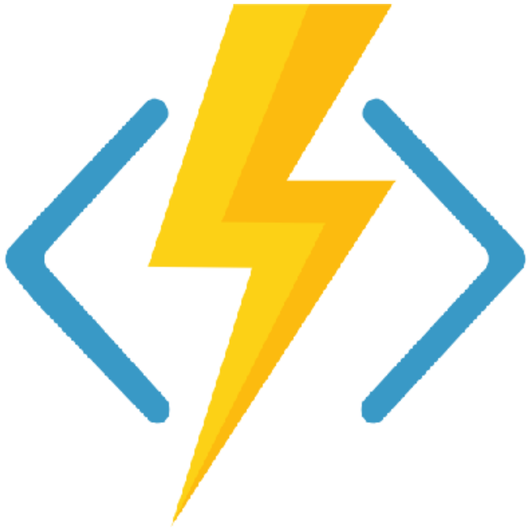
Serverless computing allows you to build and run applications and services **without thinking about servers**. Serverless applications **don't require you to provision, scale, and manage any servers**…

Building serverless applications means that your **developers can focus on their core product** instead of worrying about managing and operating servers or runtimes…

# FOCUS ON WHAT MATTERS

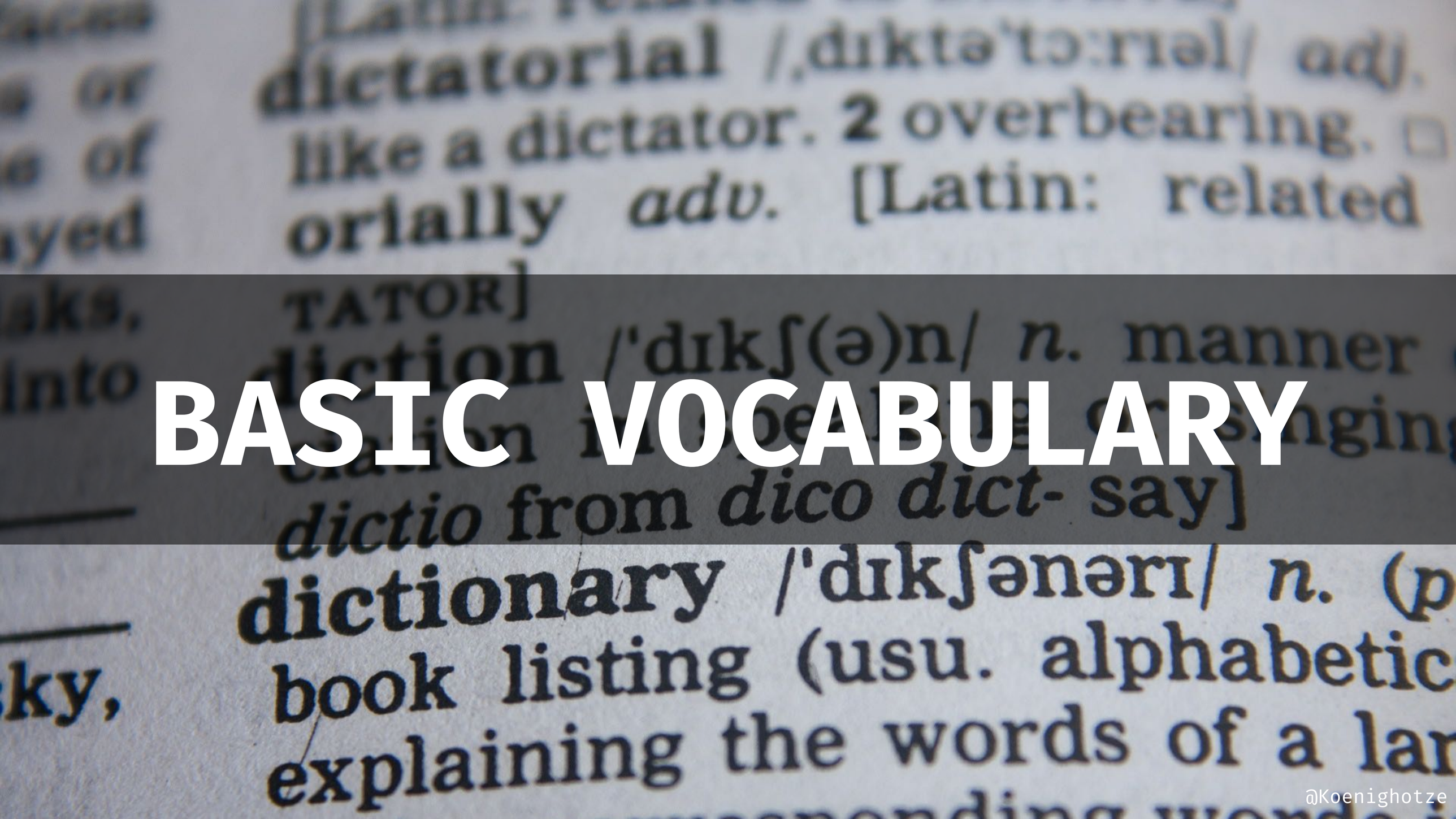

aws


webtask




APACHE
OpenWhisk


aws




# BASIC VOCABULARY

# LAMBDA

# –

# SERVERLESS COMPUTE

# S3

# –

# DROPBOX

# IAM

# –

# SECURITY

# CLOUDFORMATION

# –

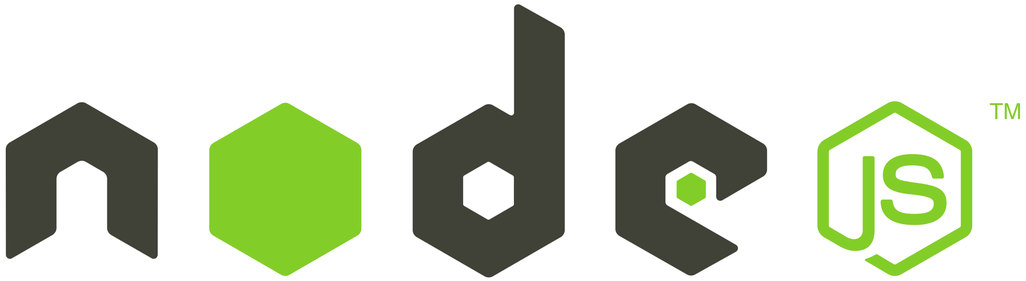
# PROVISIONING

# WHAT IS A “LAMBDA FUNCTION”?

Event driven

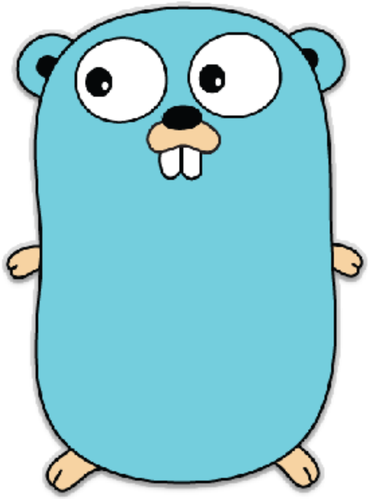
Stateless  Single purpose

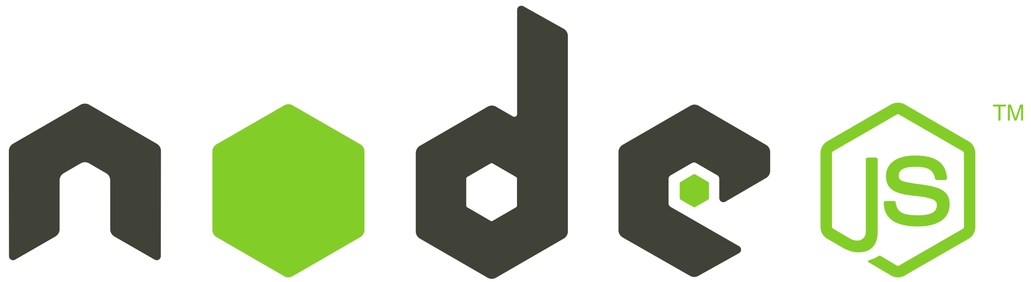
Asynchronous



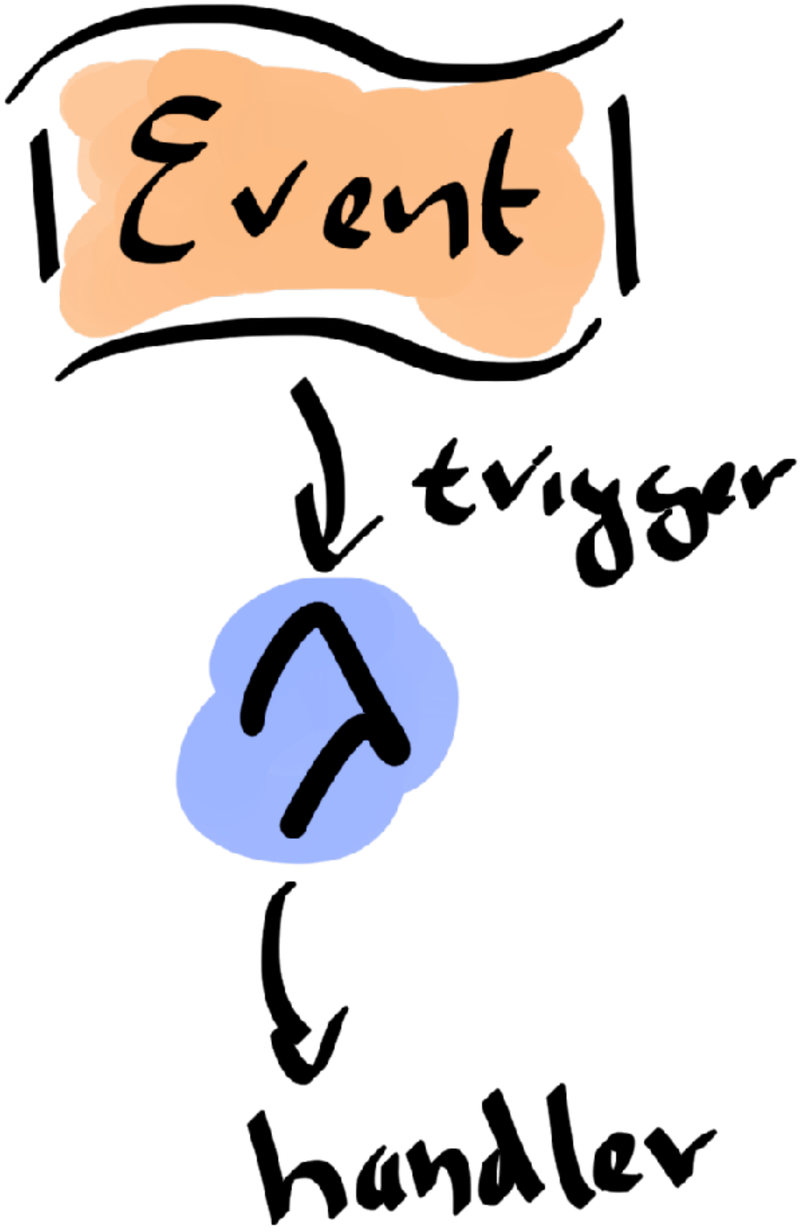

C#

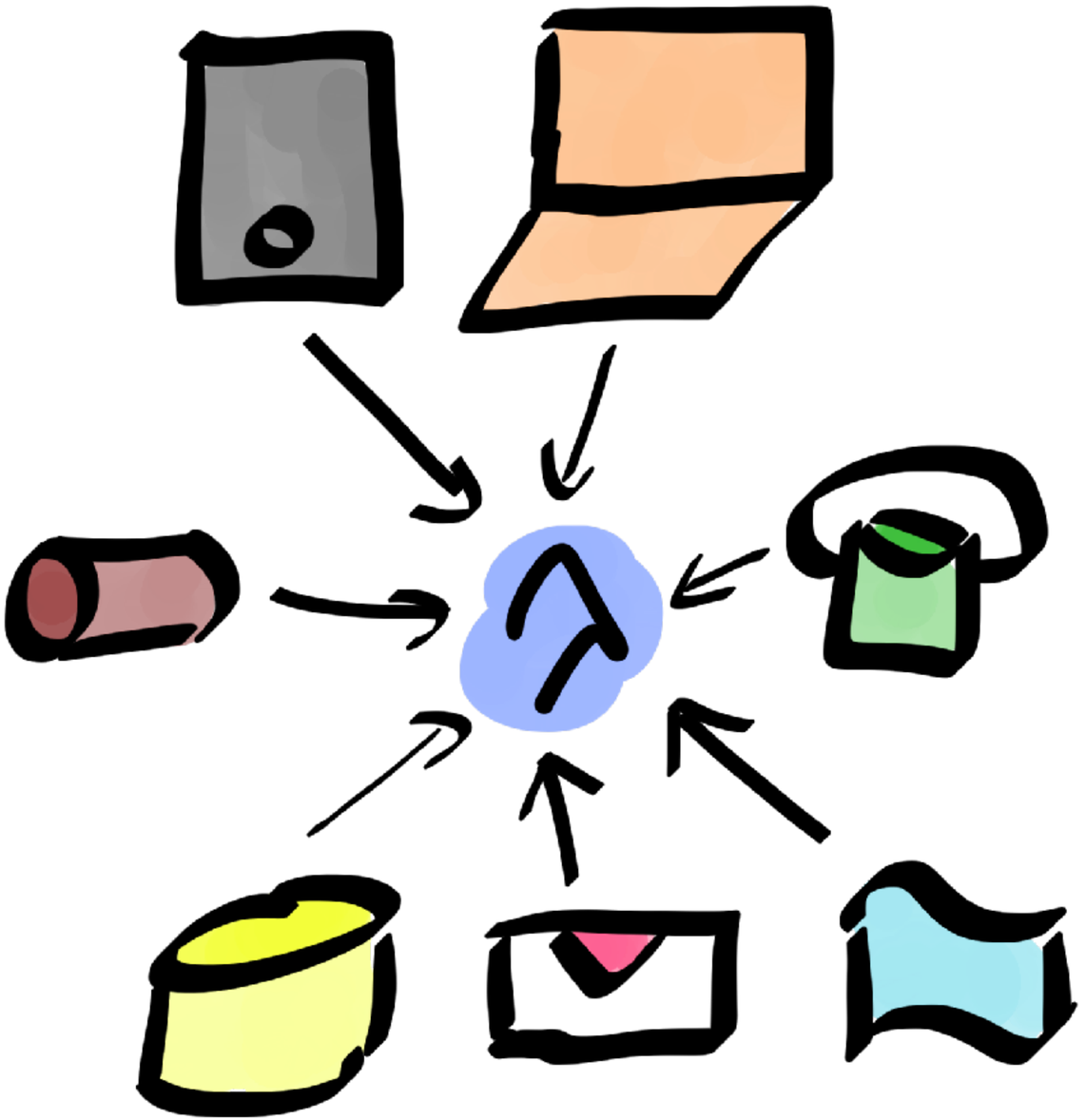
Java™




node
JS
TM

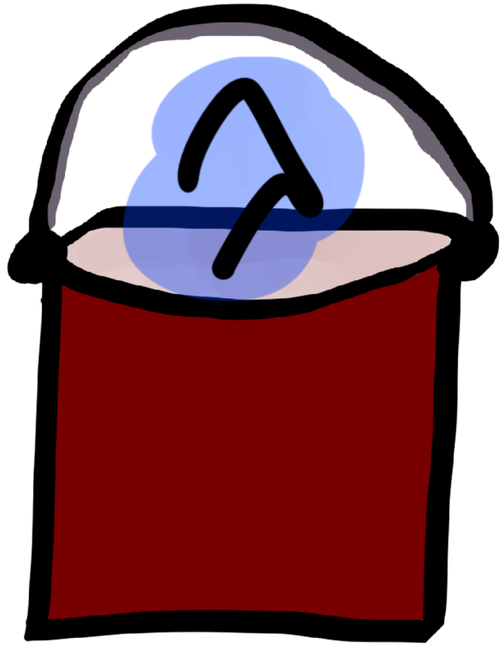
# EXECUTION MODEL

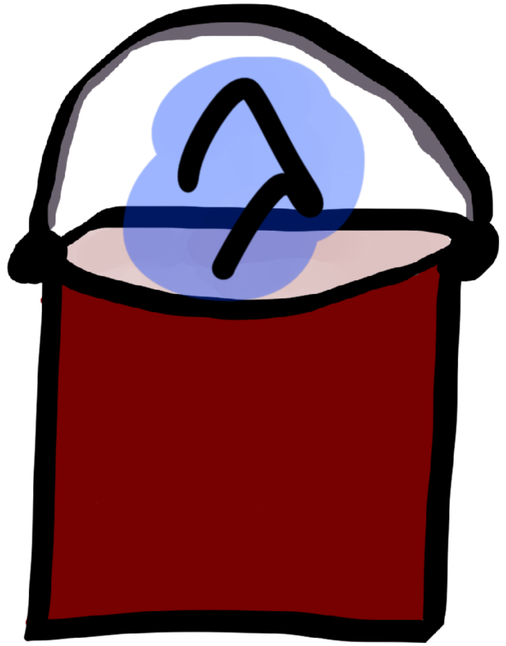

Event
trigger
λ
handler

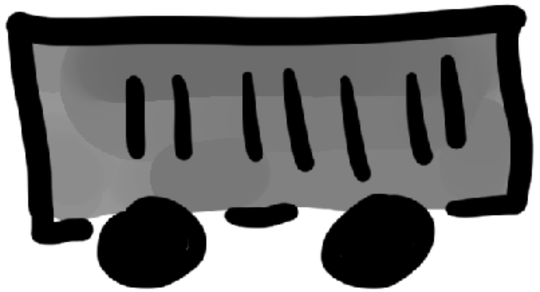


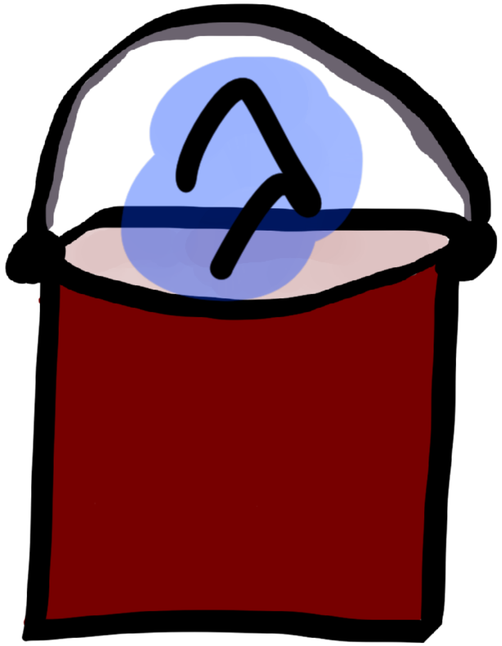

S3

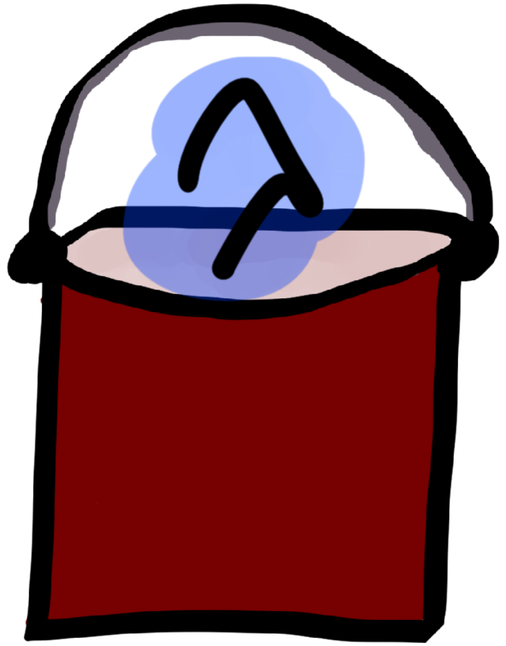

Event

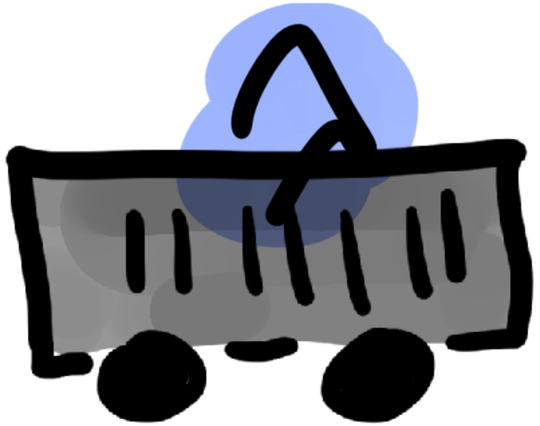


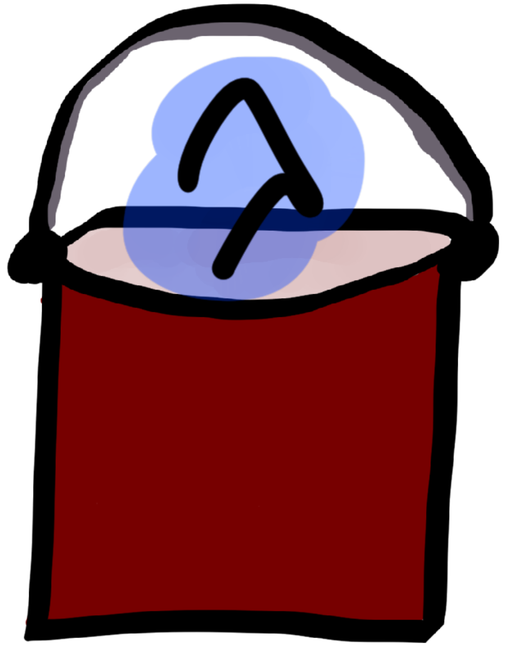




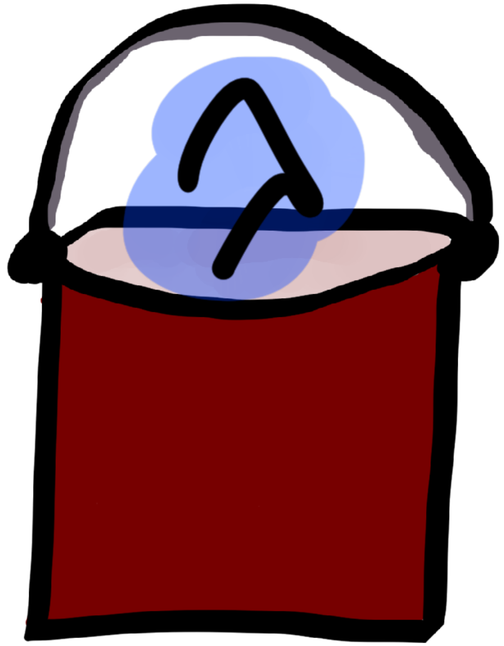


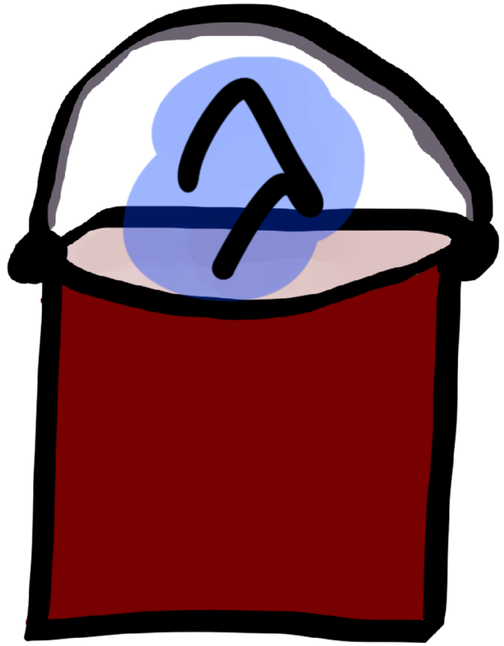




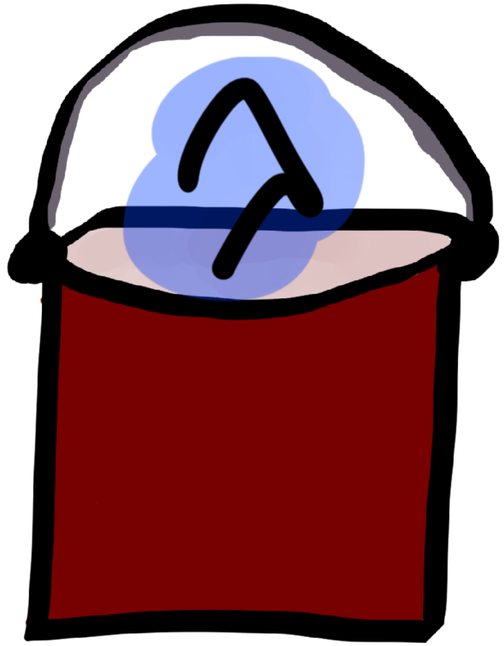


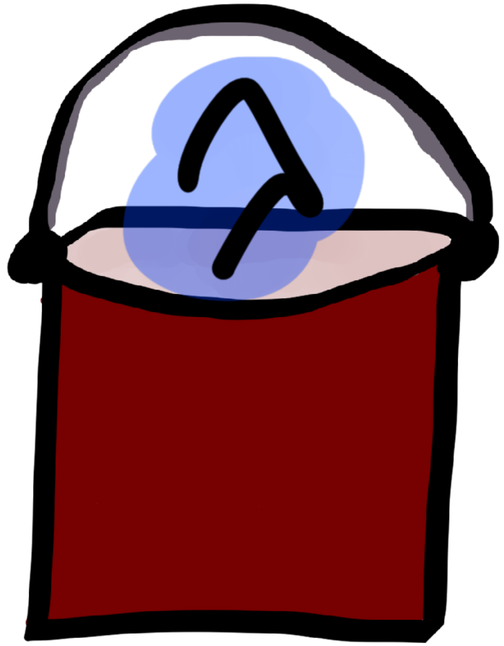

Event

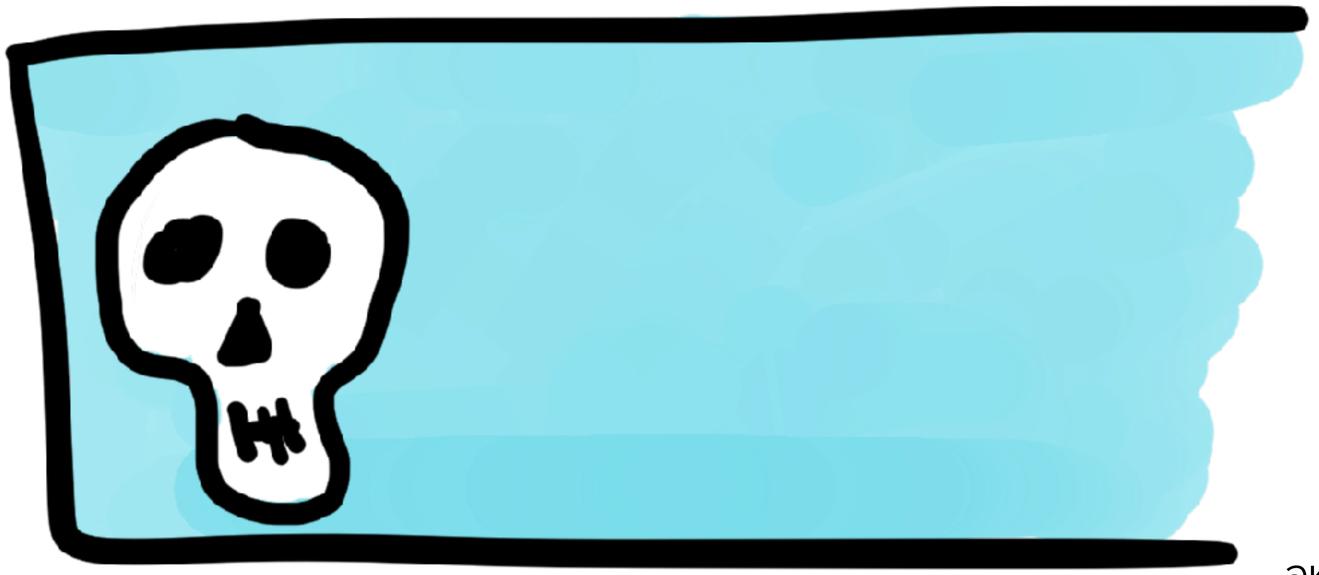


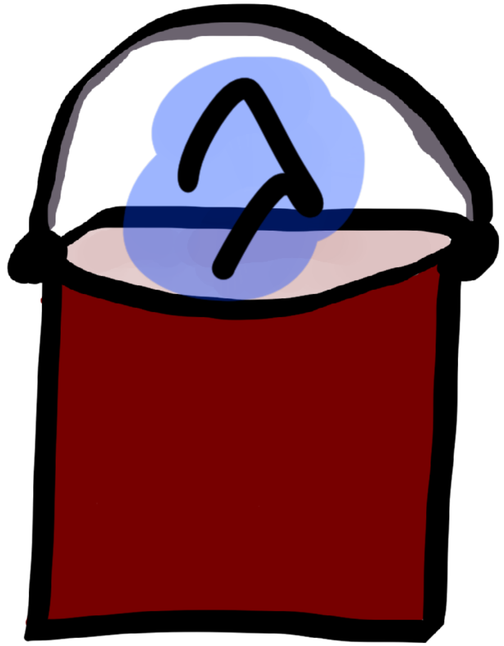


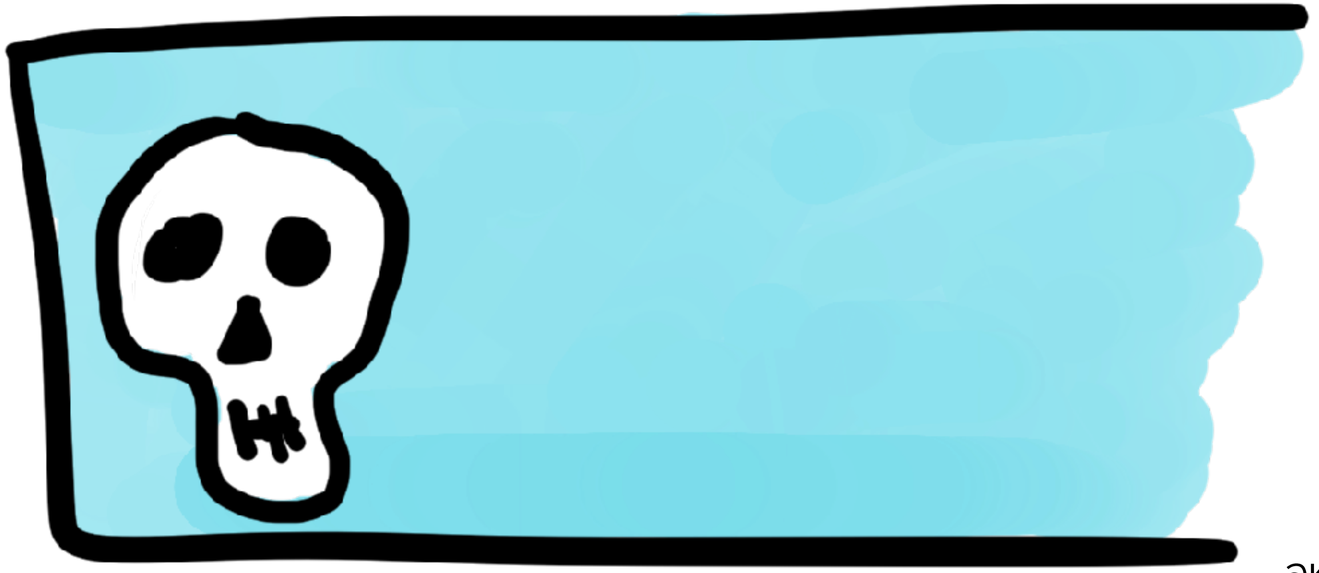
# Some time later…









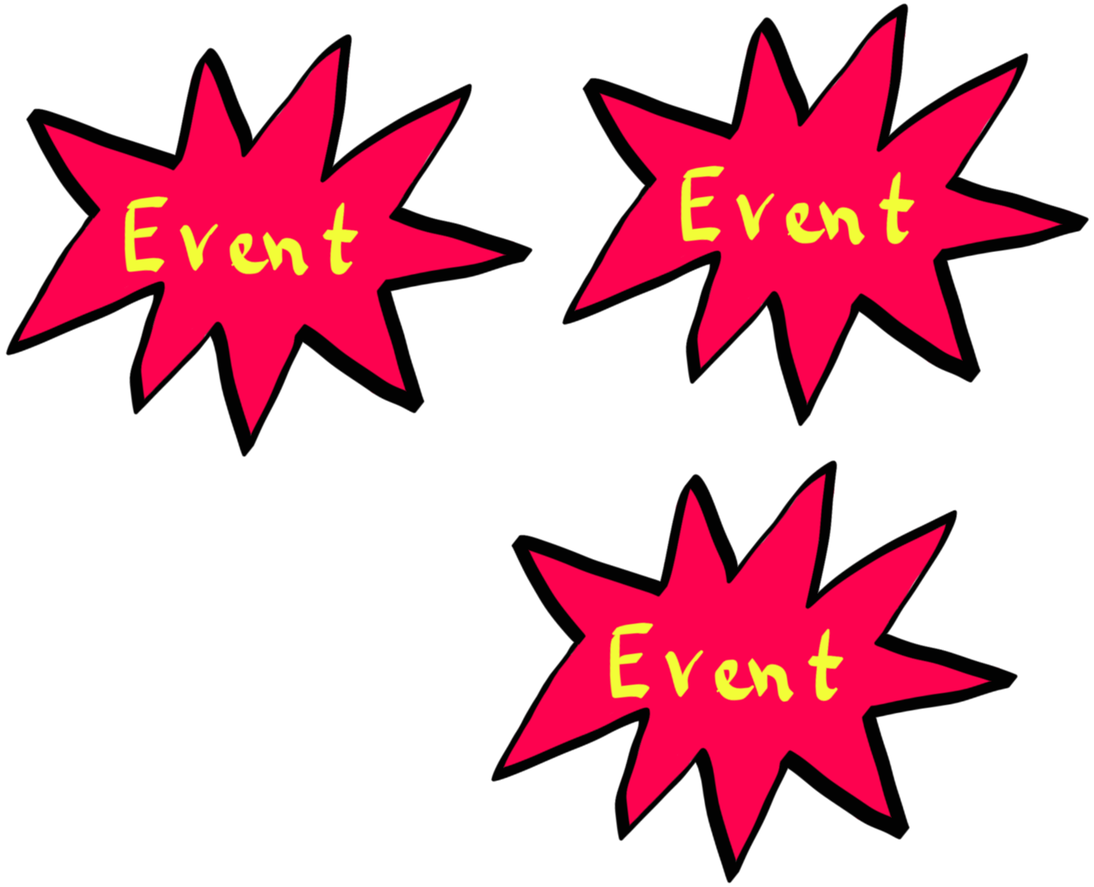


# SCALE BY REQUEST


Event

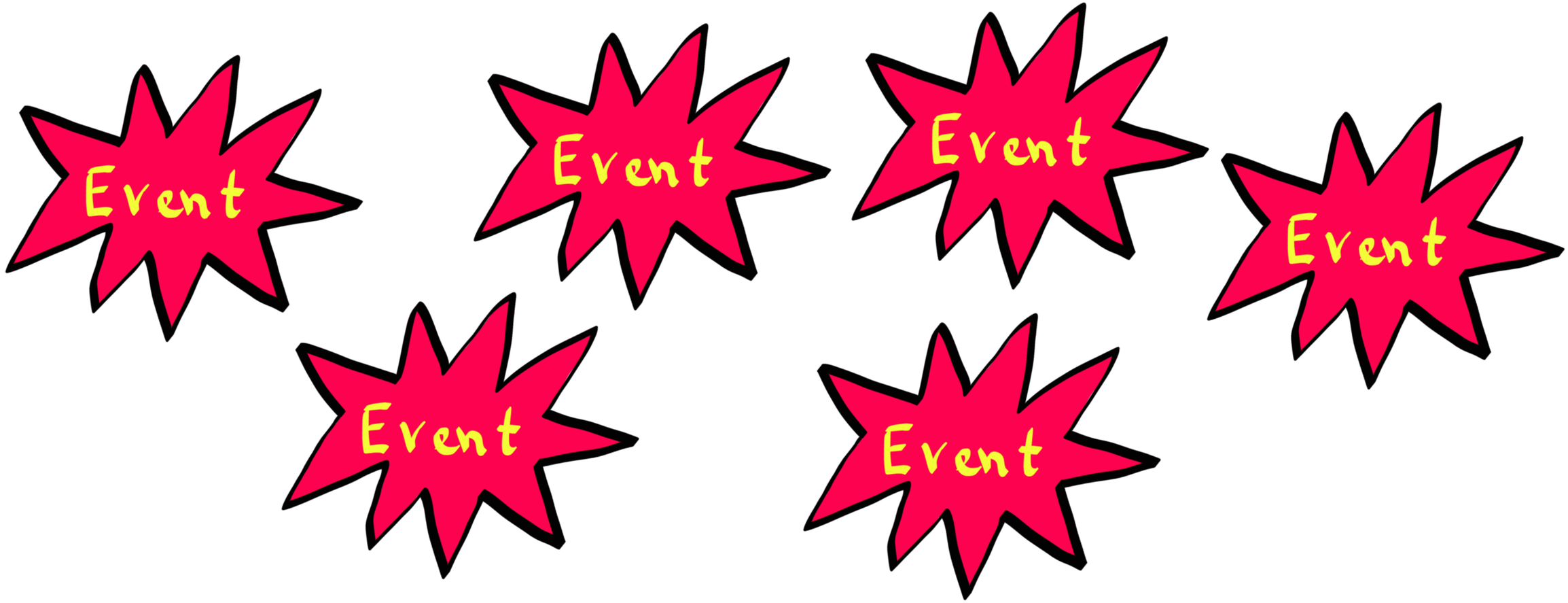

Event

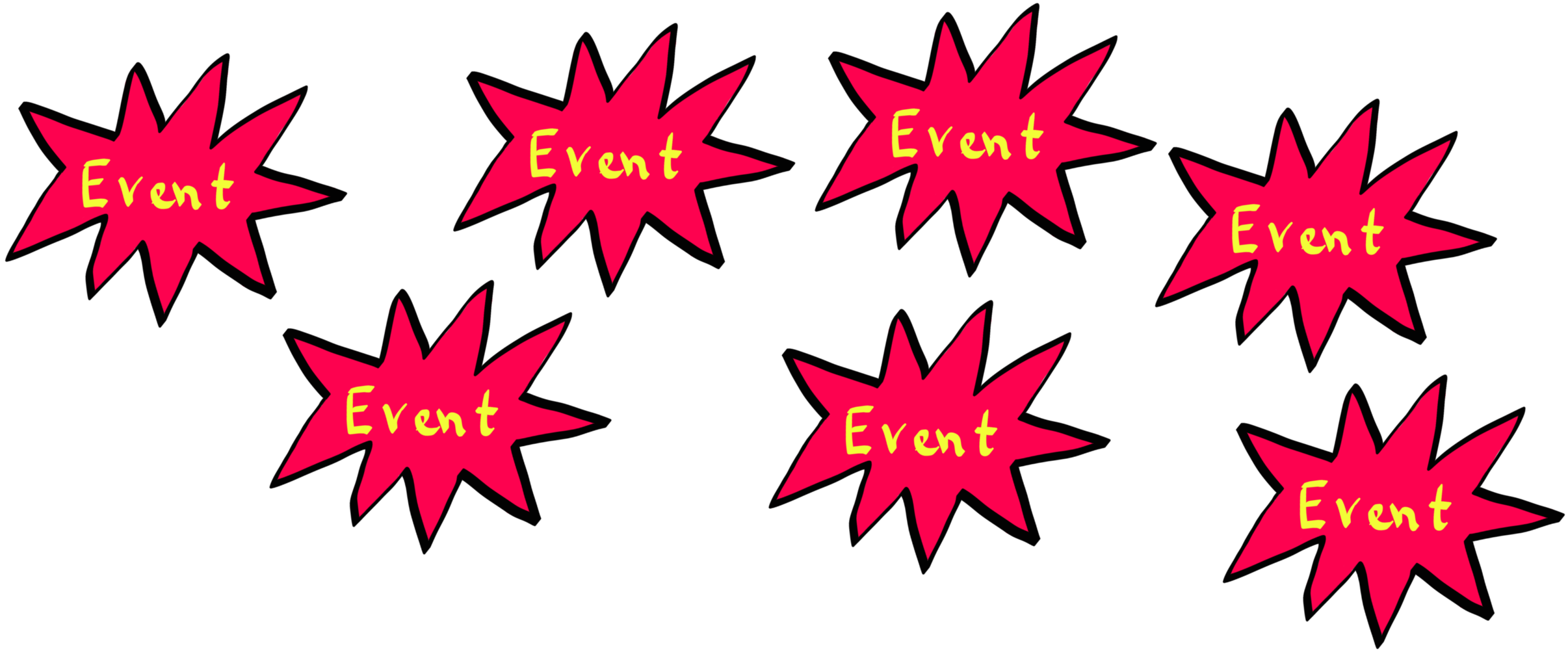

Event

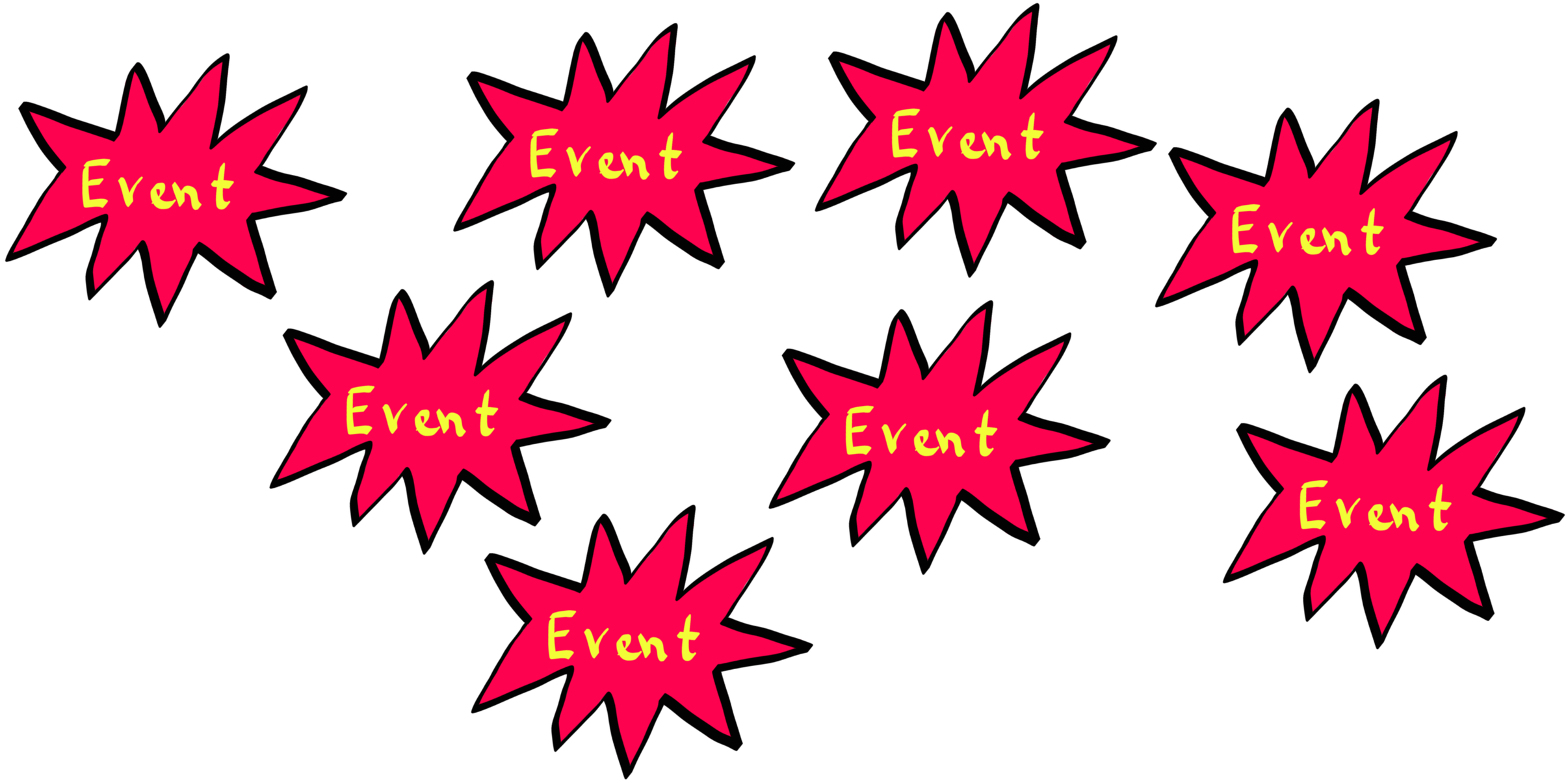

Event
Event
Event

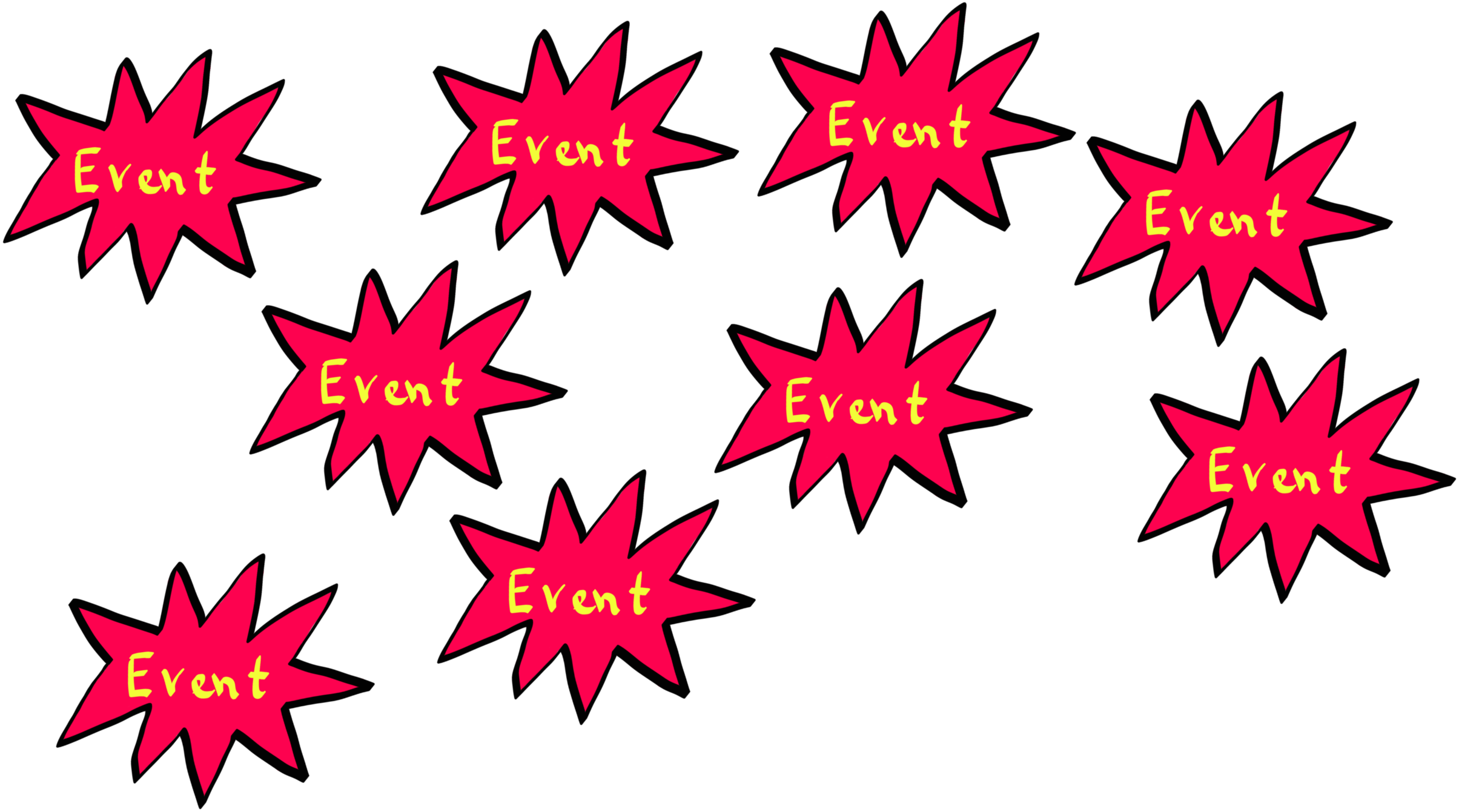

Event
Event
Event
Event

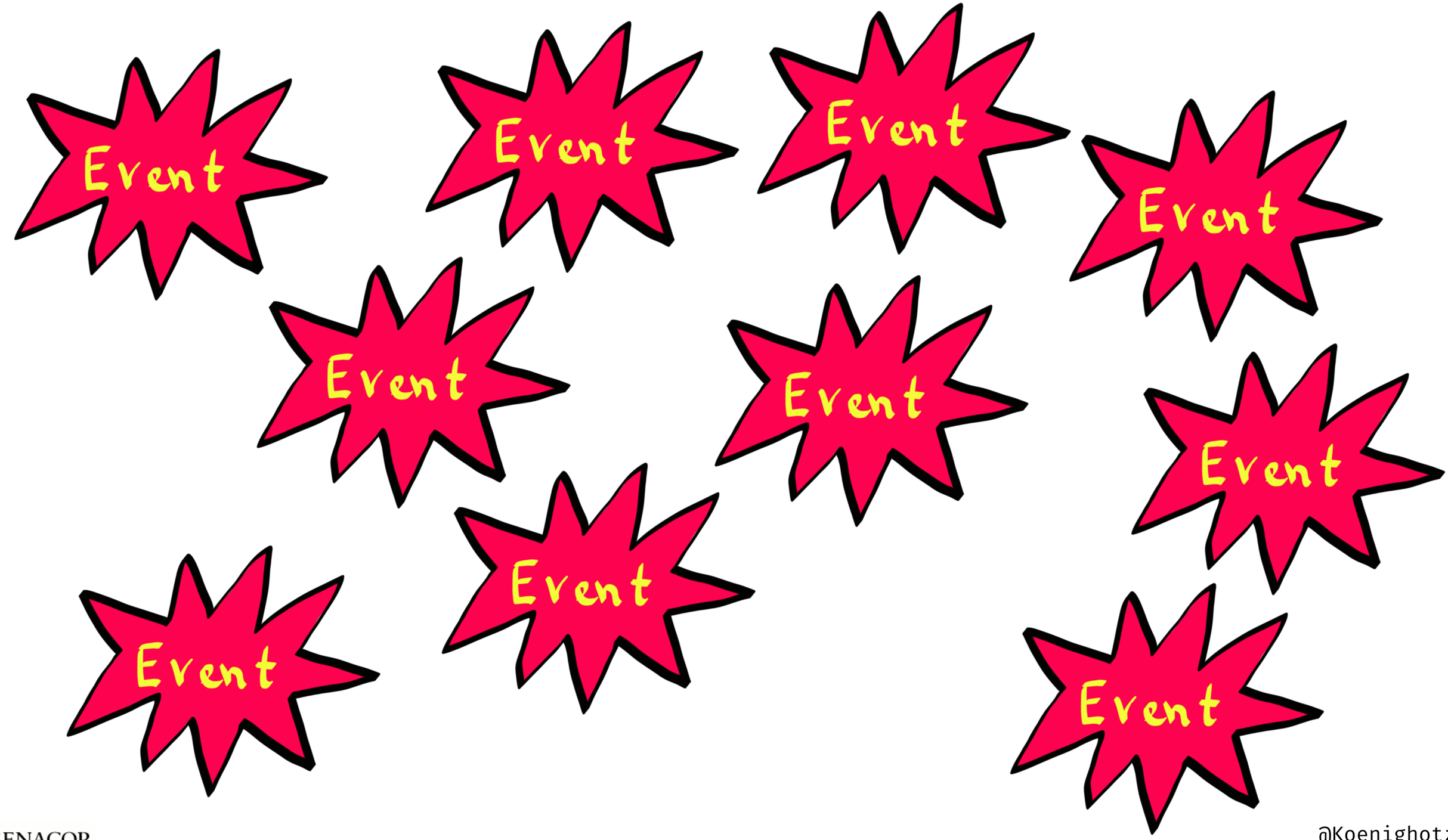

Event
Event
Event
Event
Event

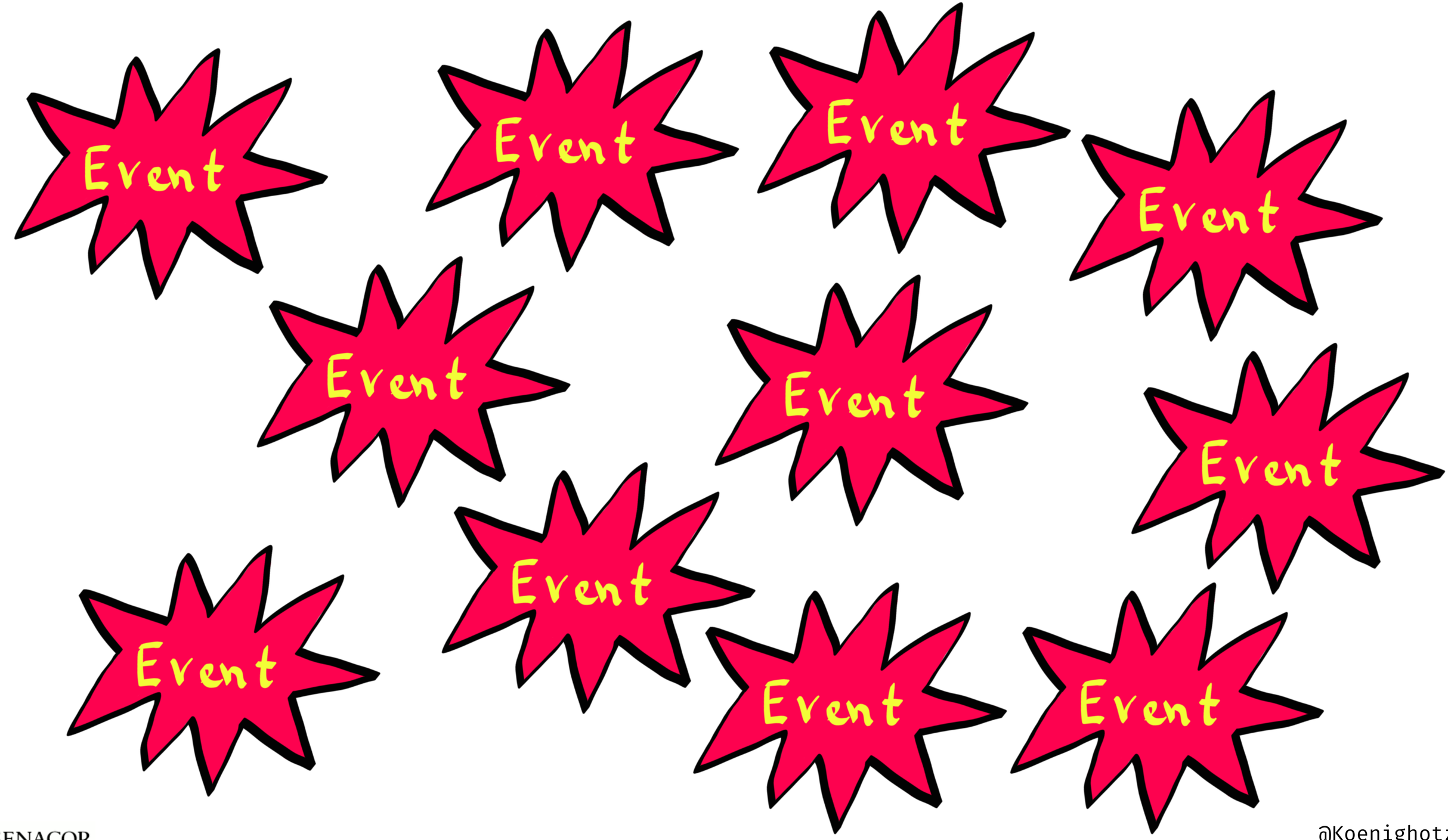

Event
Event
Event
Event
Event
Event

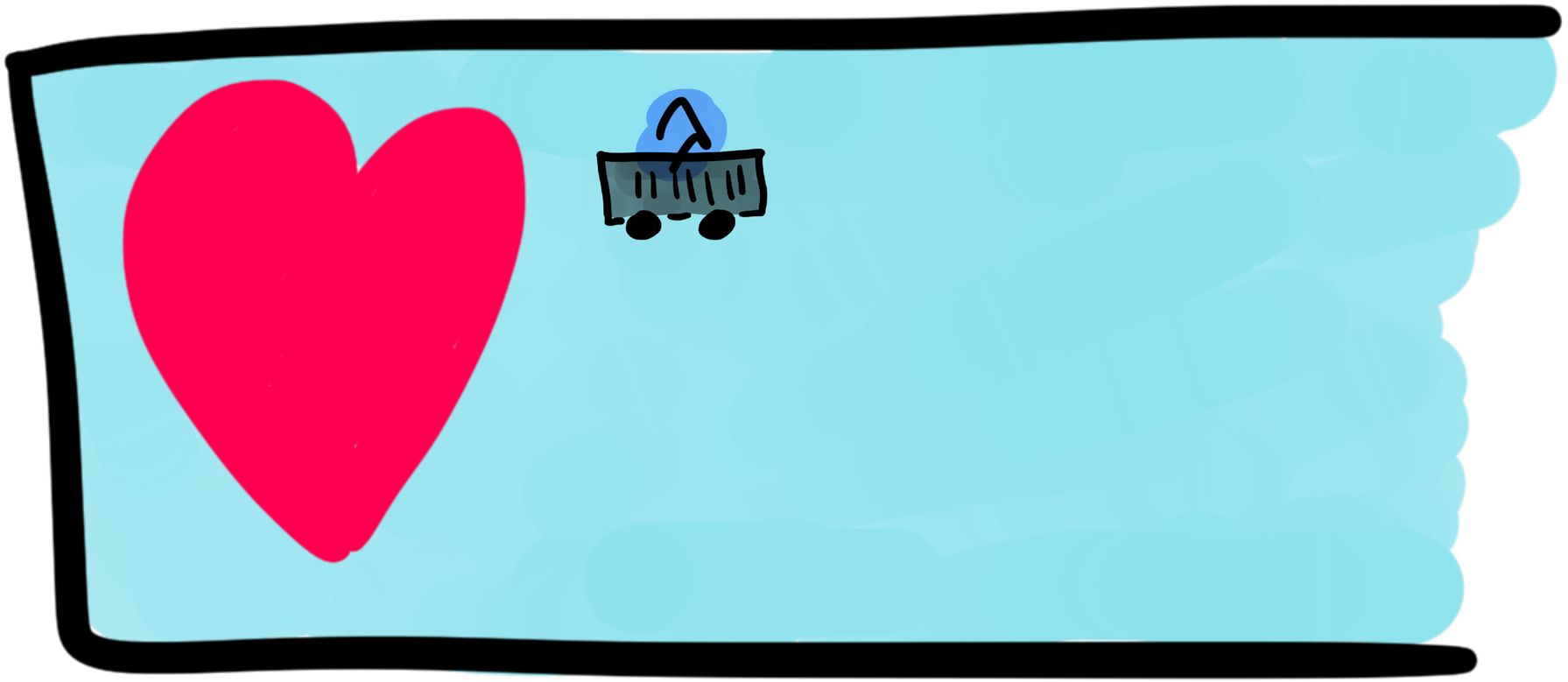

Event
Event
Event
Event
Event
Event
Event

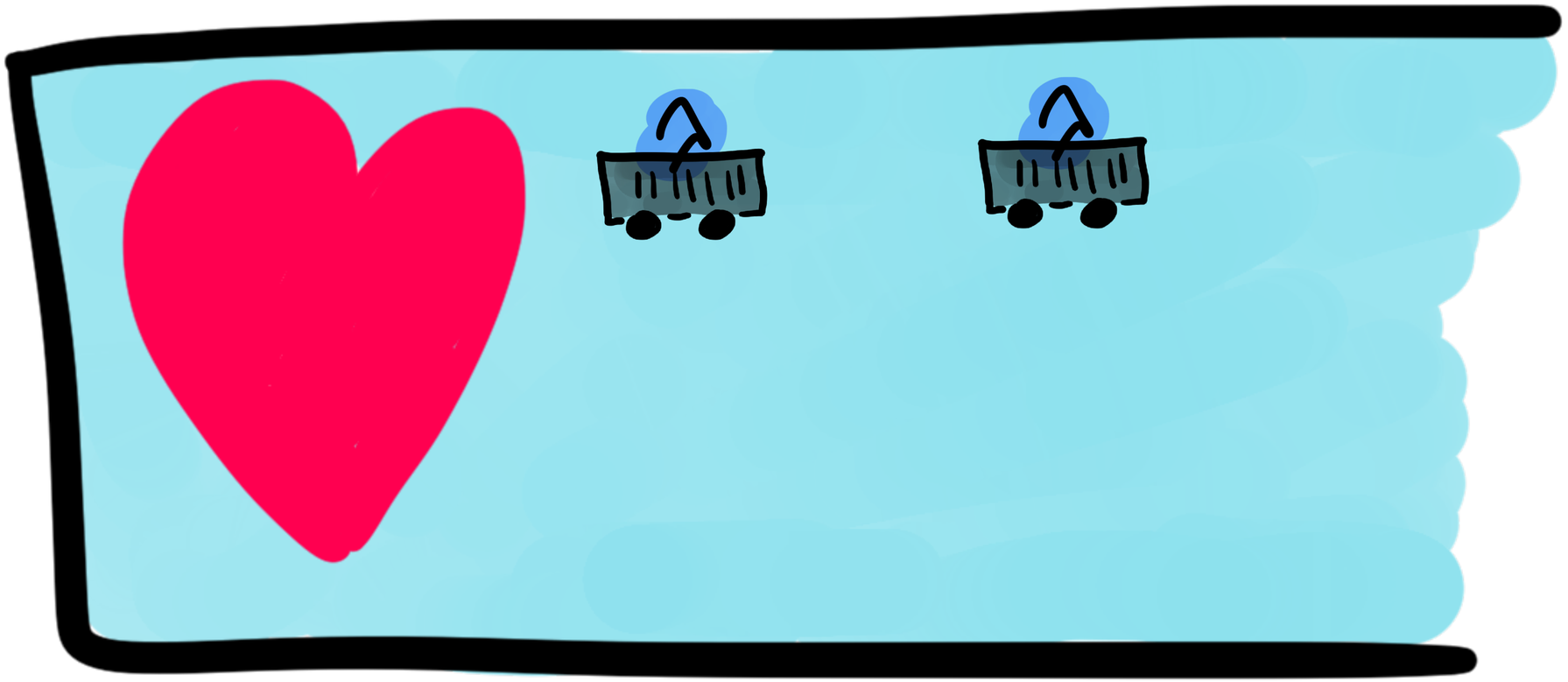

Event
Event
Event
Event
Event
Event
Event
Event

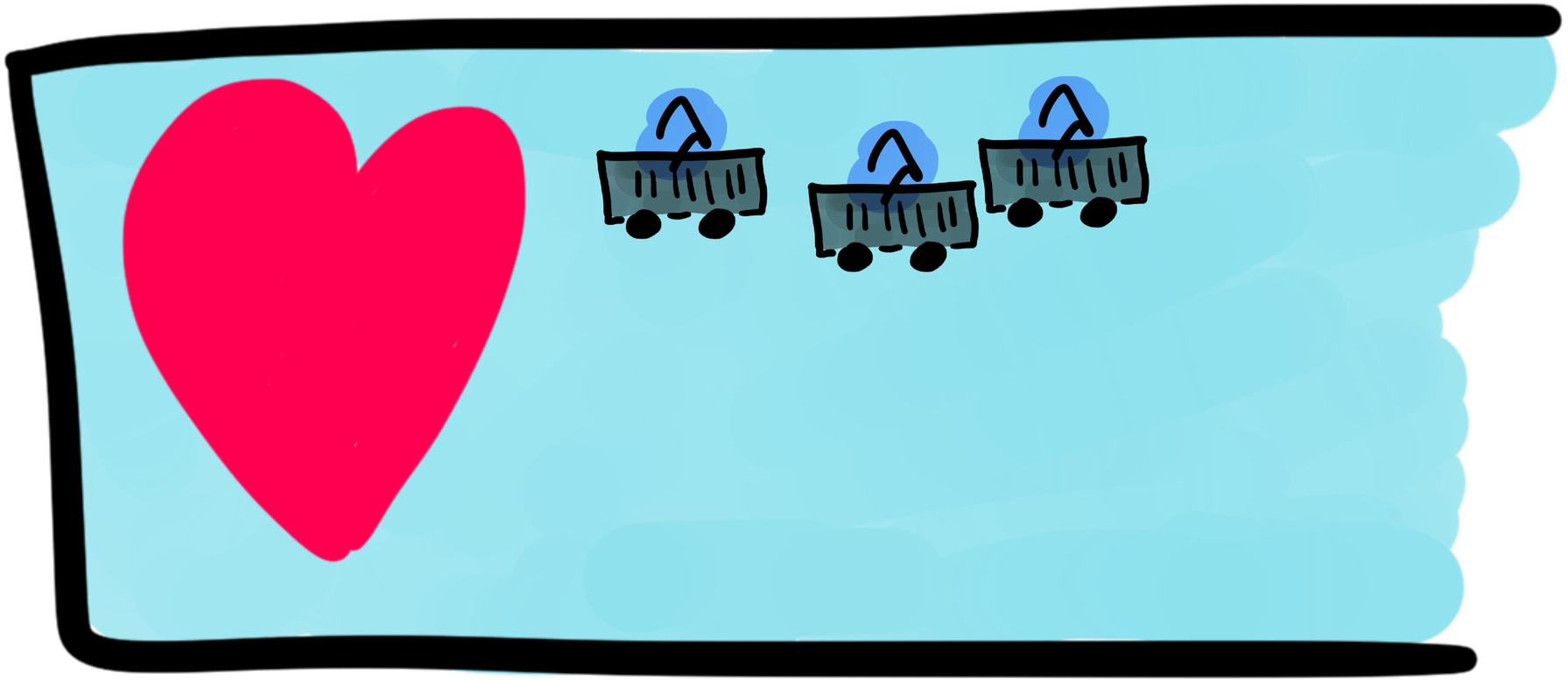

Event
Event
Event
Event
Event
Event
Event
Event
Event

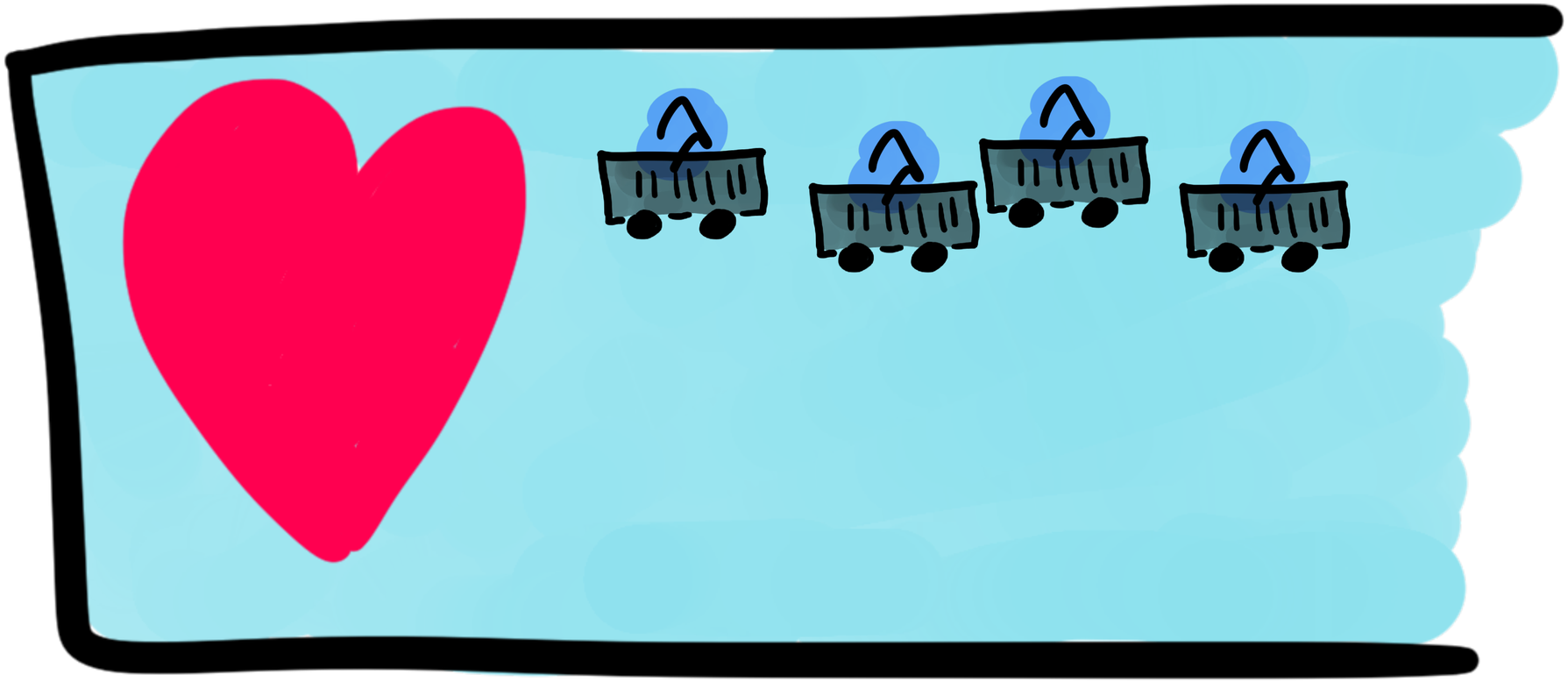

Event
Event
Event
Event
Event
Event
Event
Event
Event
Event
Event

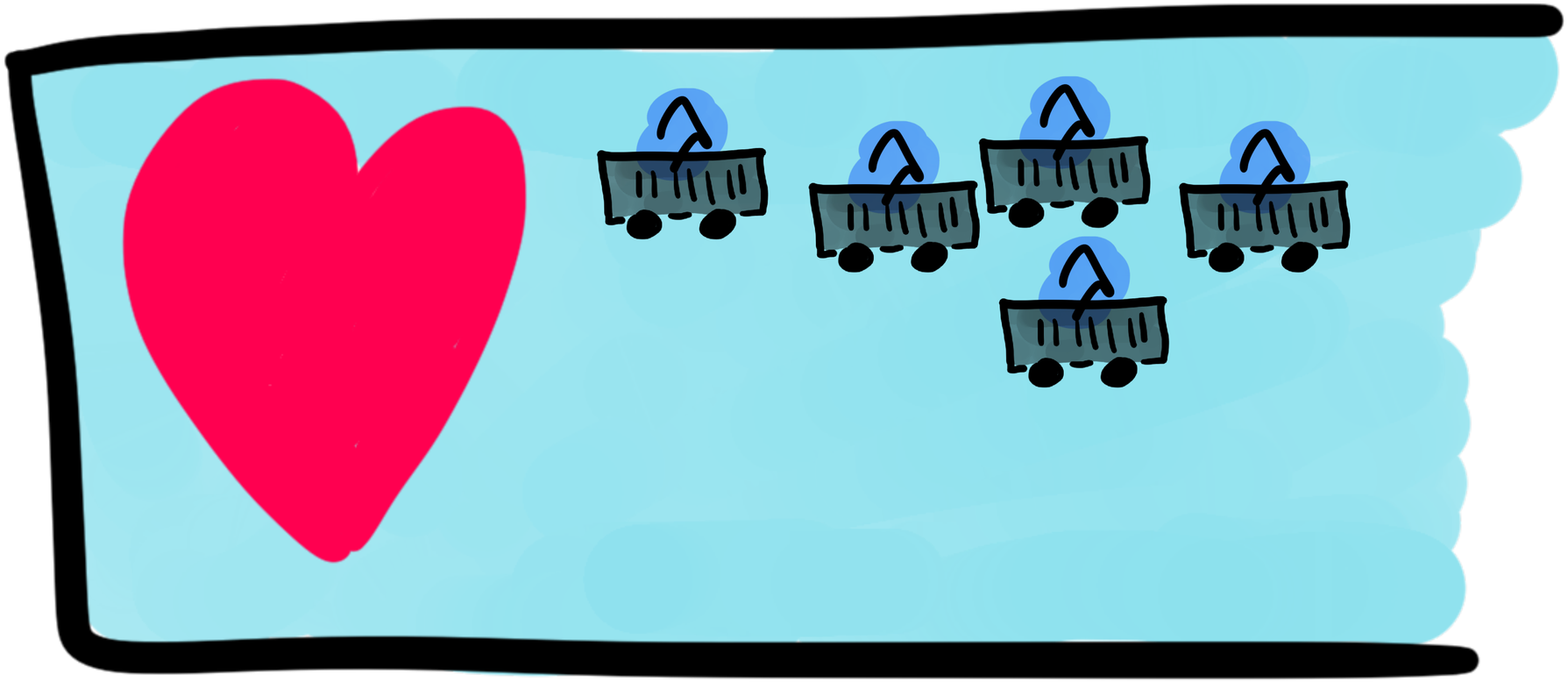

Event
Event
Event
Event
Event
Event
Event
Event
Event
Event
Event
Event

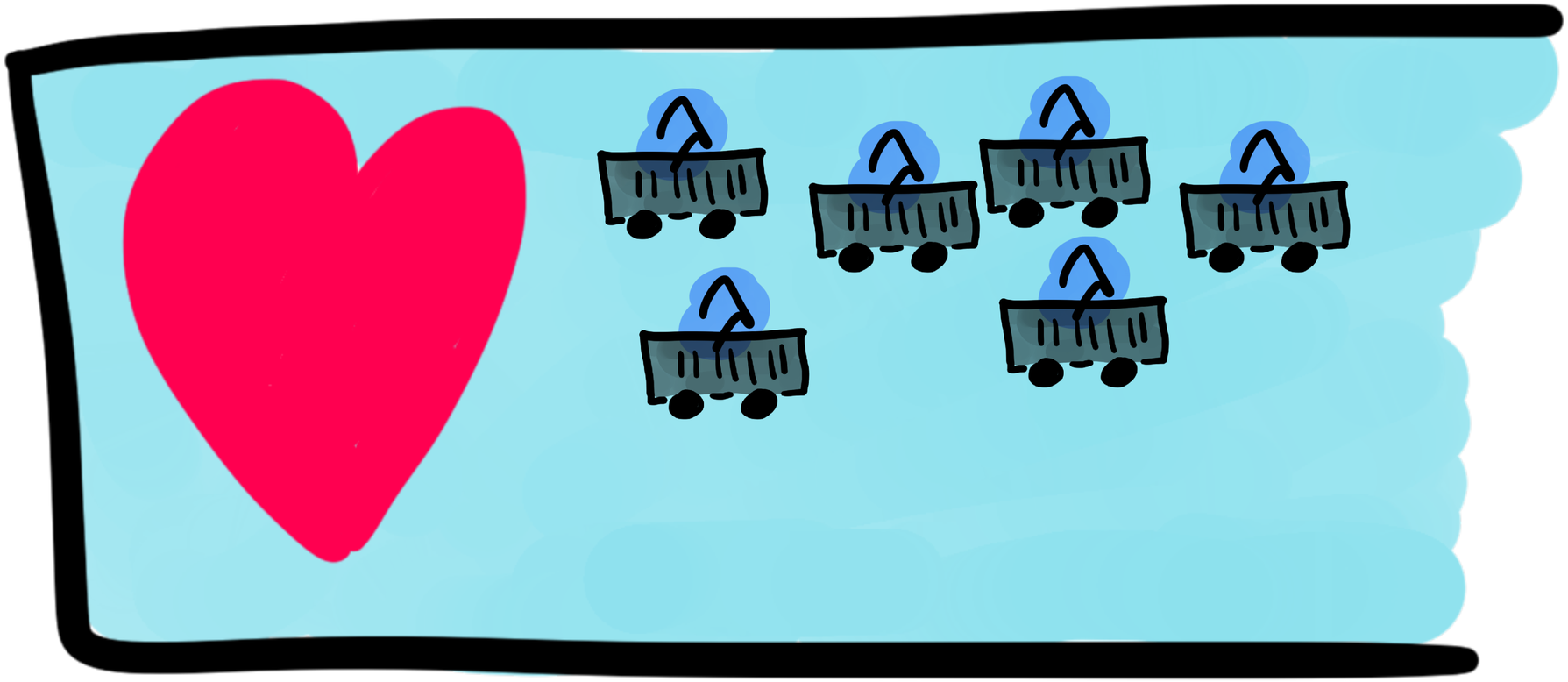


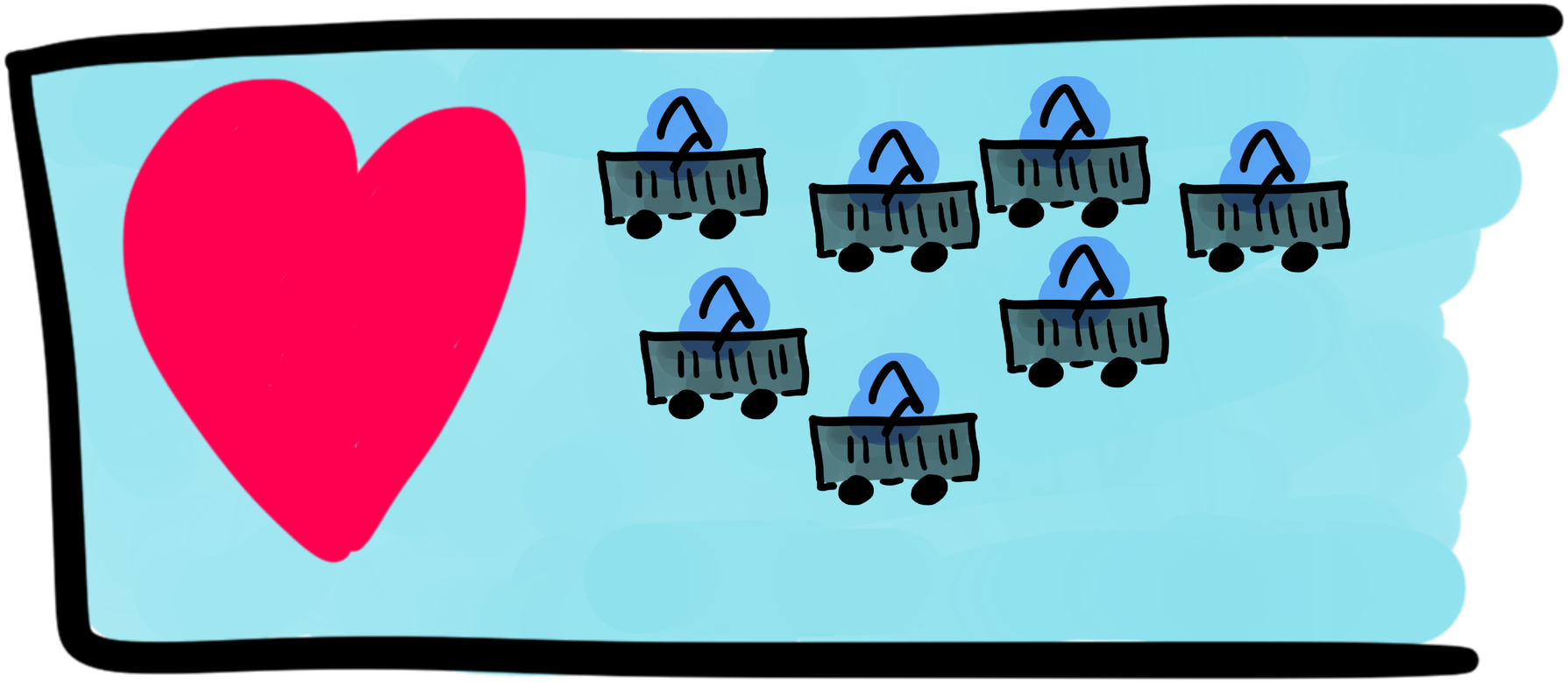


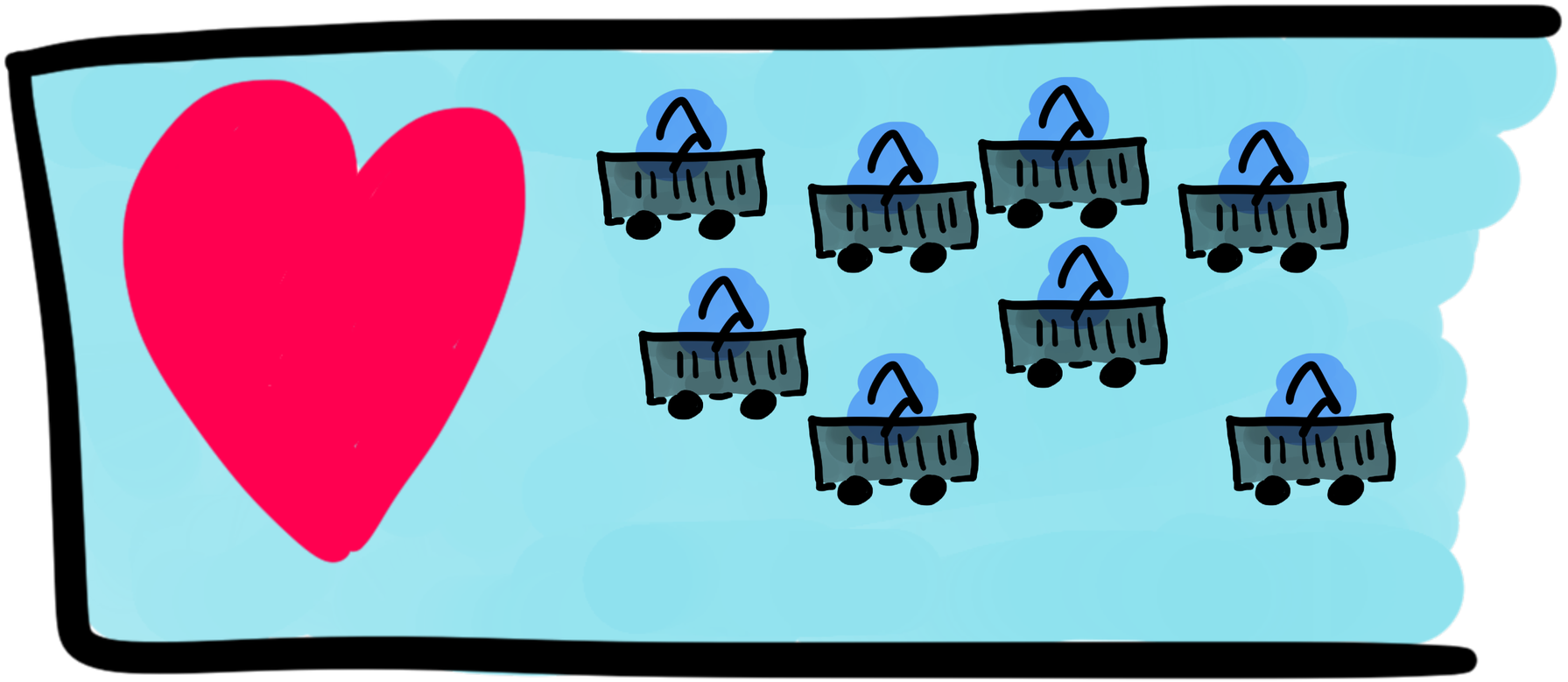


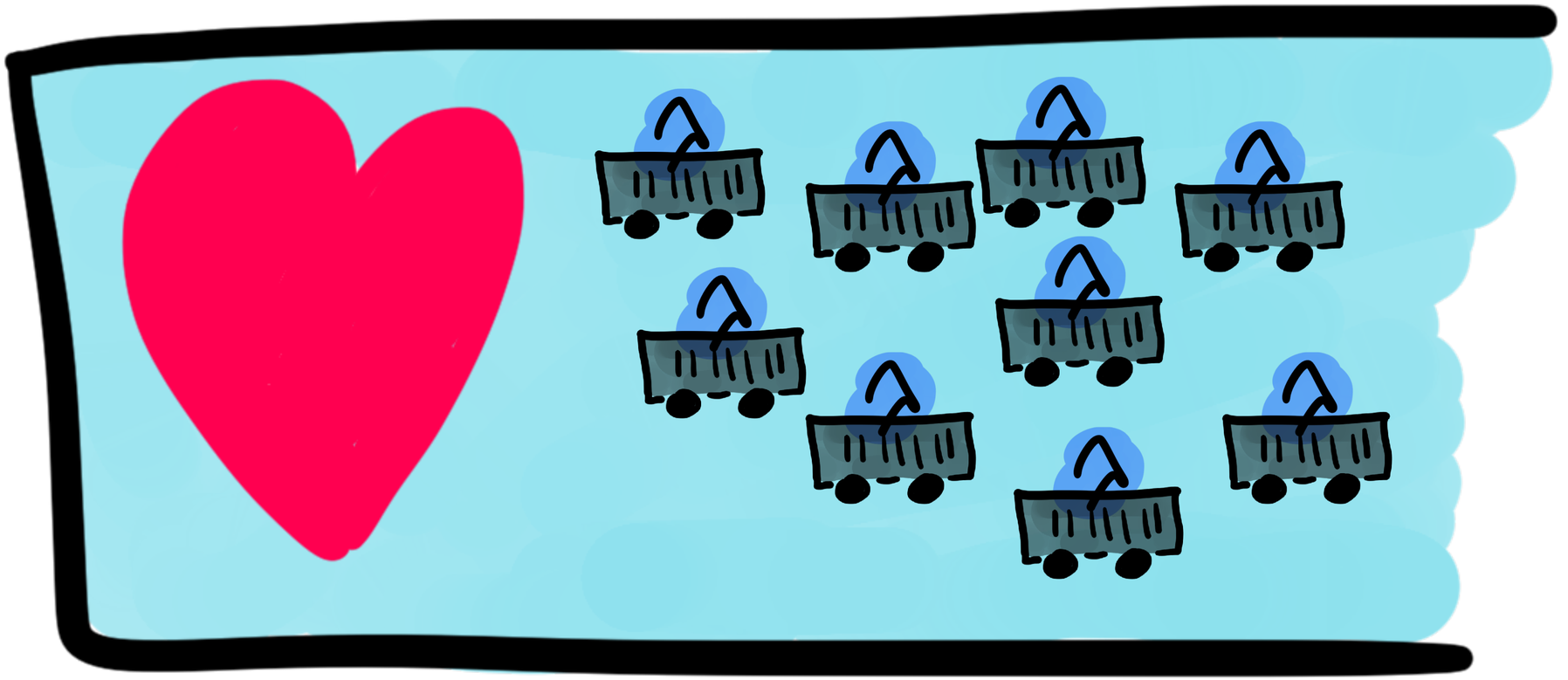


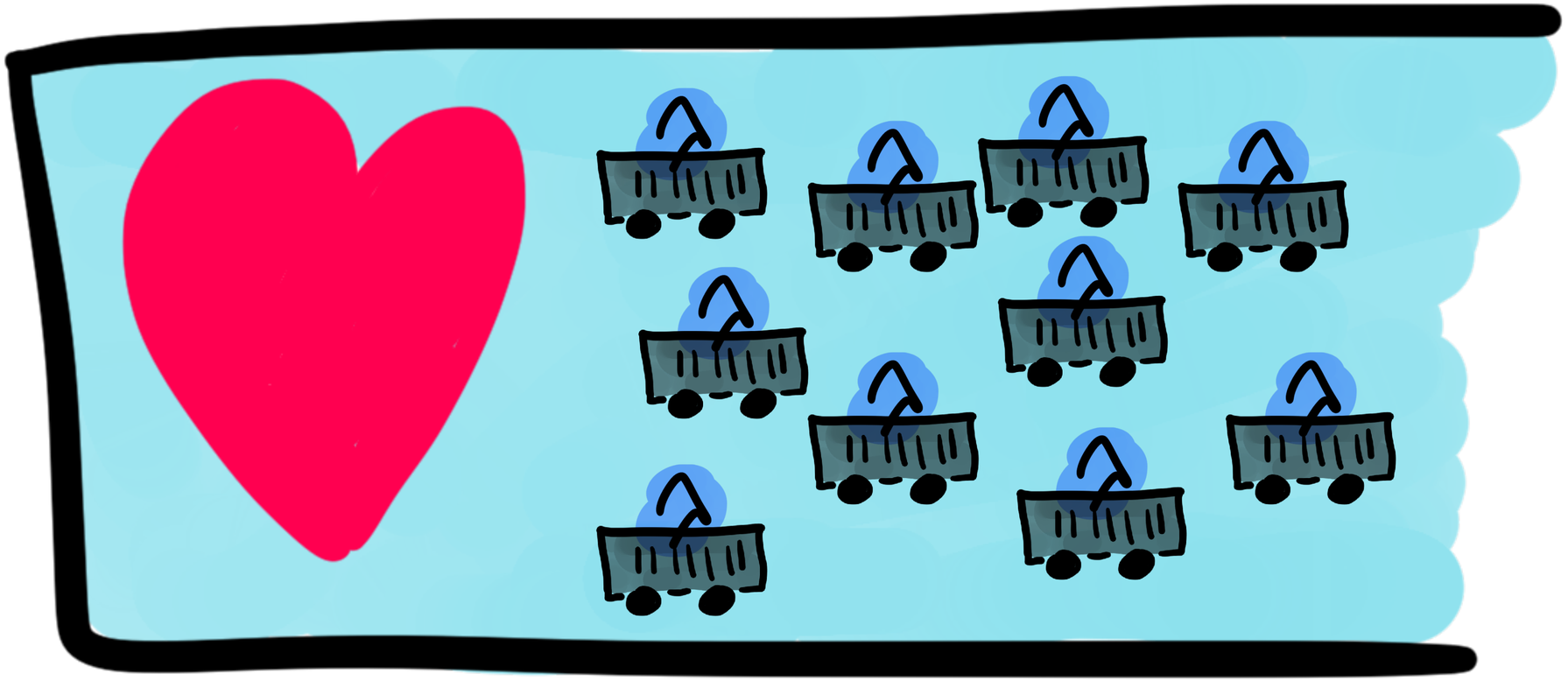






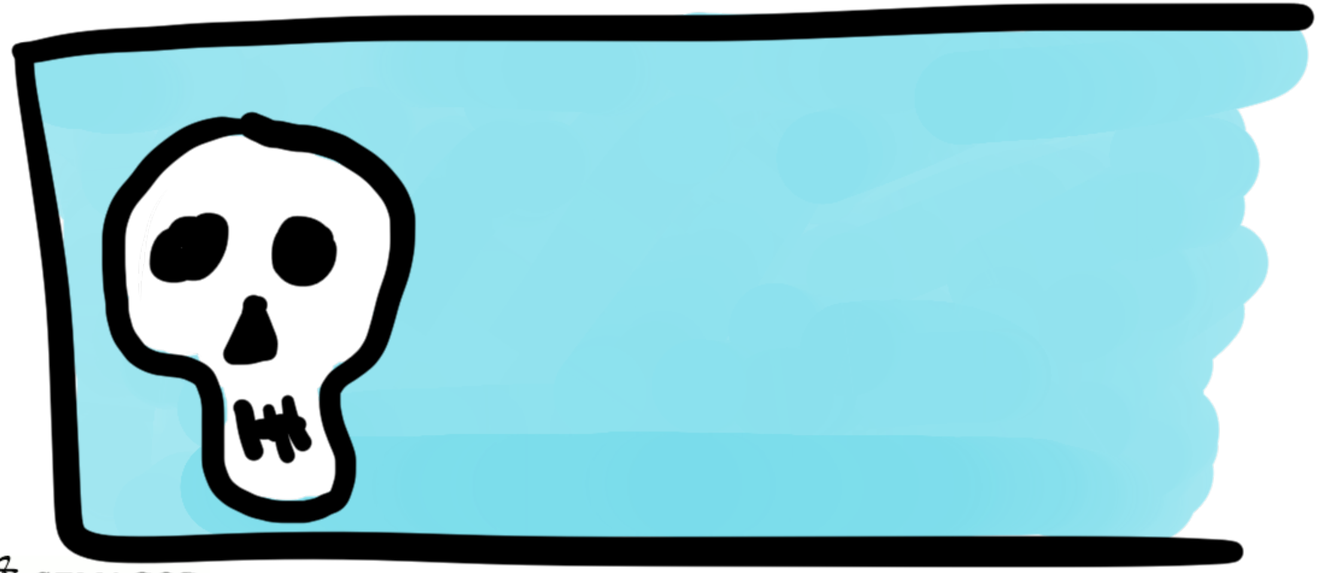




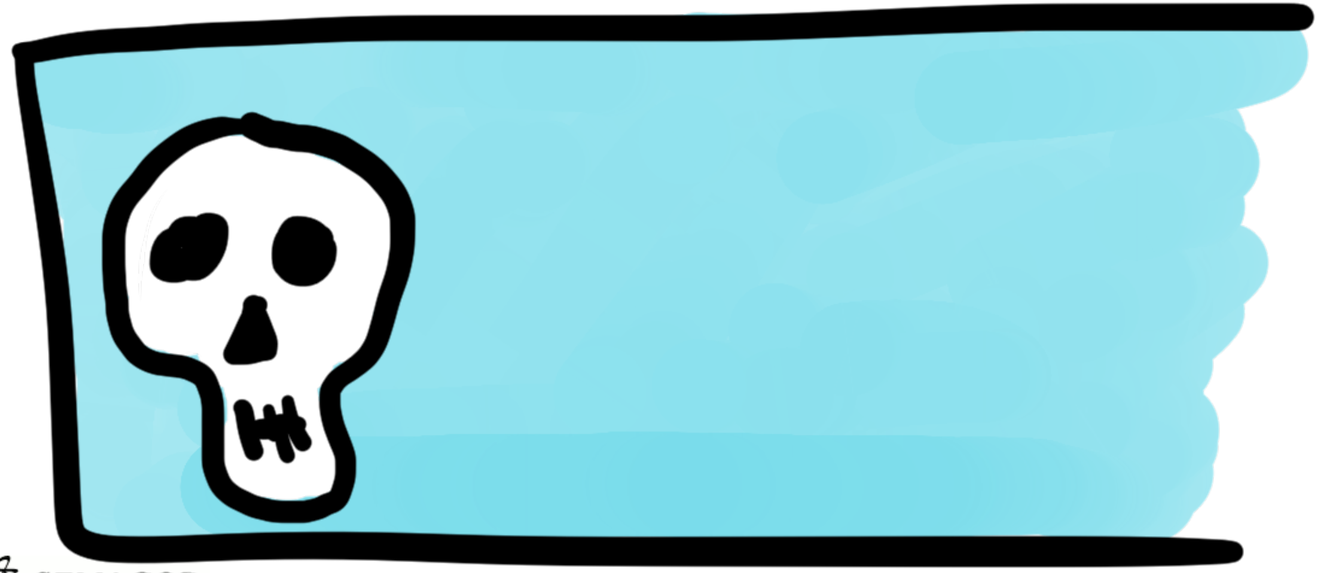


# NO OVERPROVISION
# NO UNDERPROVISION


# CHARGE BY EXECUTION




# CHARGE BY EXECUTION




FRAMEWORKS, RUNTIMES
AND TOOLS
@Koenighotze


Apex

Chalice


Claudia.js

Serverless Express


Serverless Framework

Serverless Java Container


Sparta


Zappa

# AWS LAMBDA MAY NEED

# NO SPECIAL FRAMEWORK

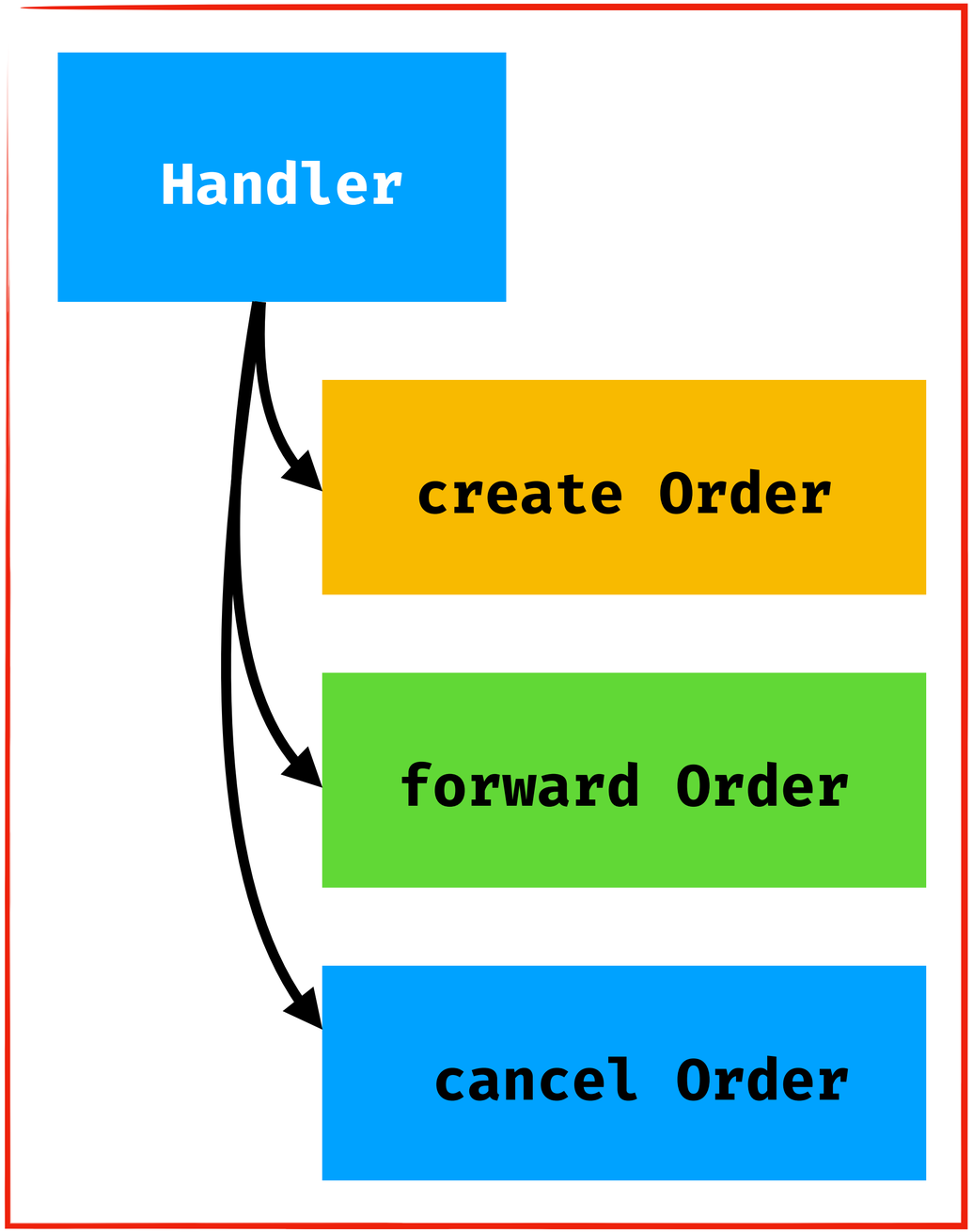
# VENDOR LOCK-IN

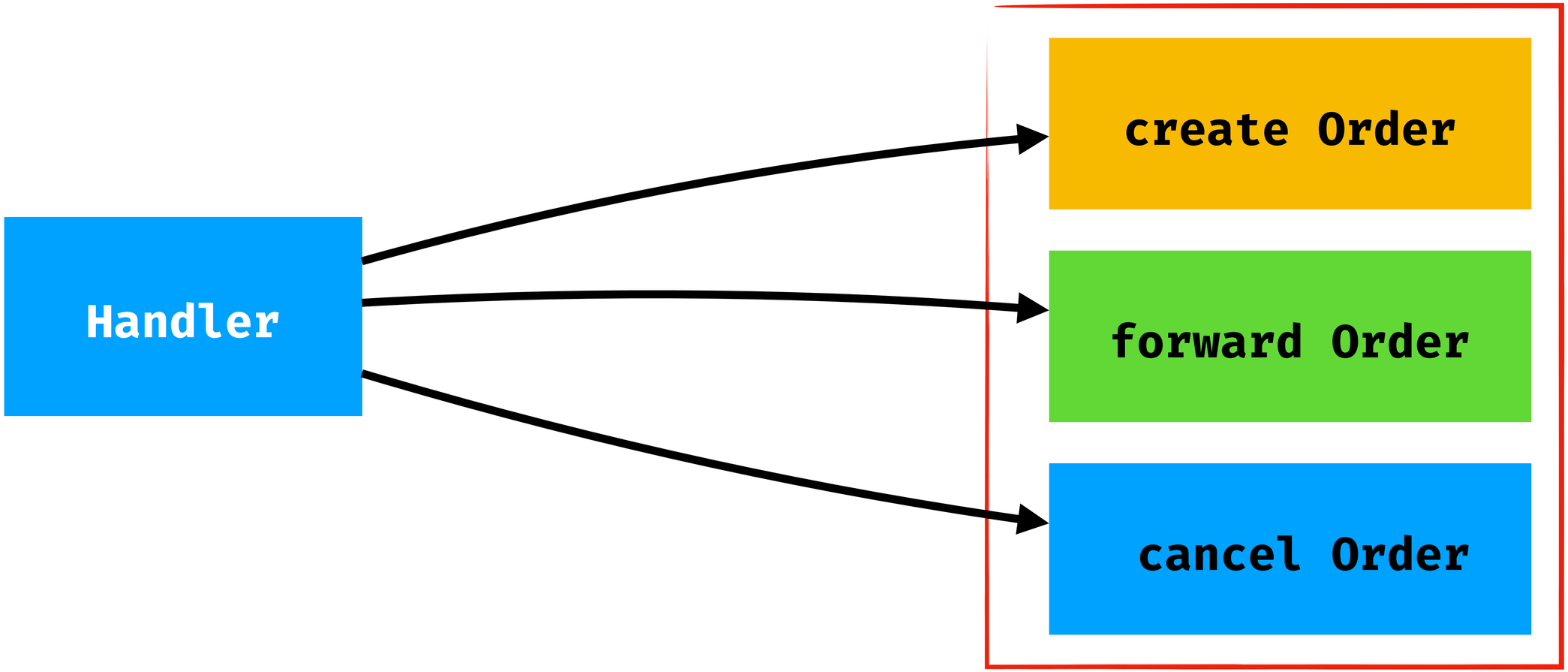
# LOG4J

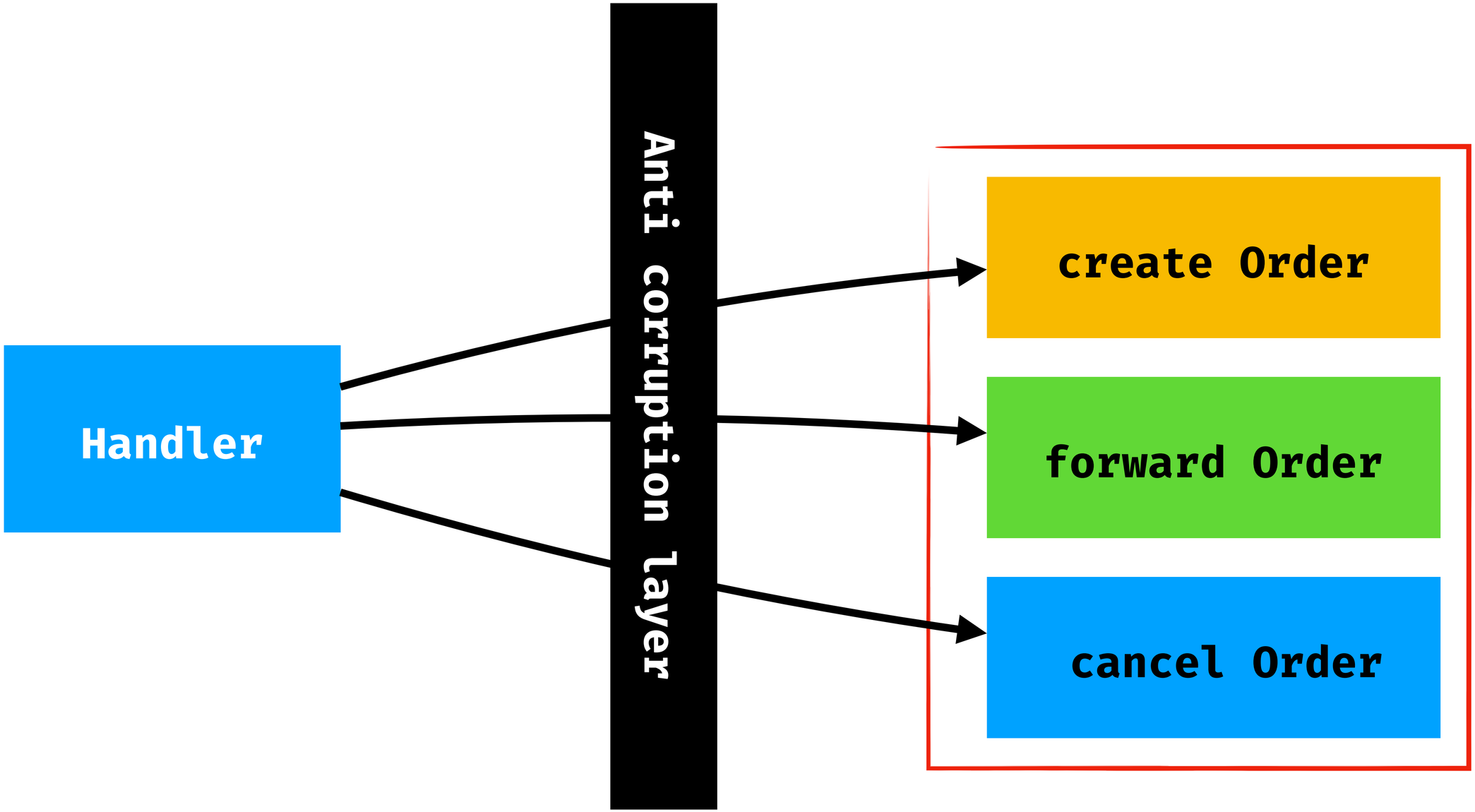
# VS.

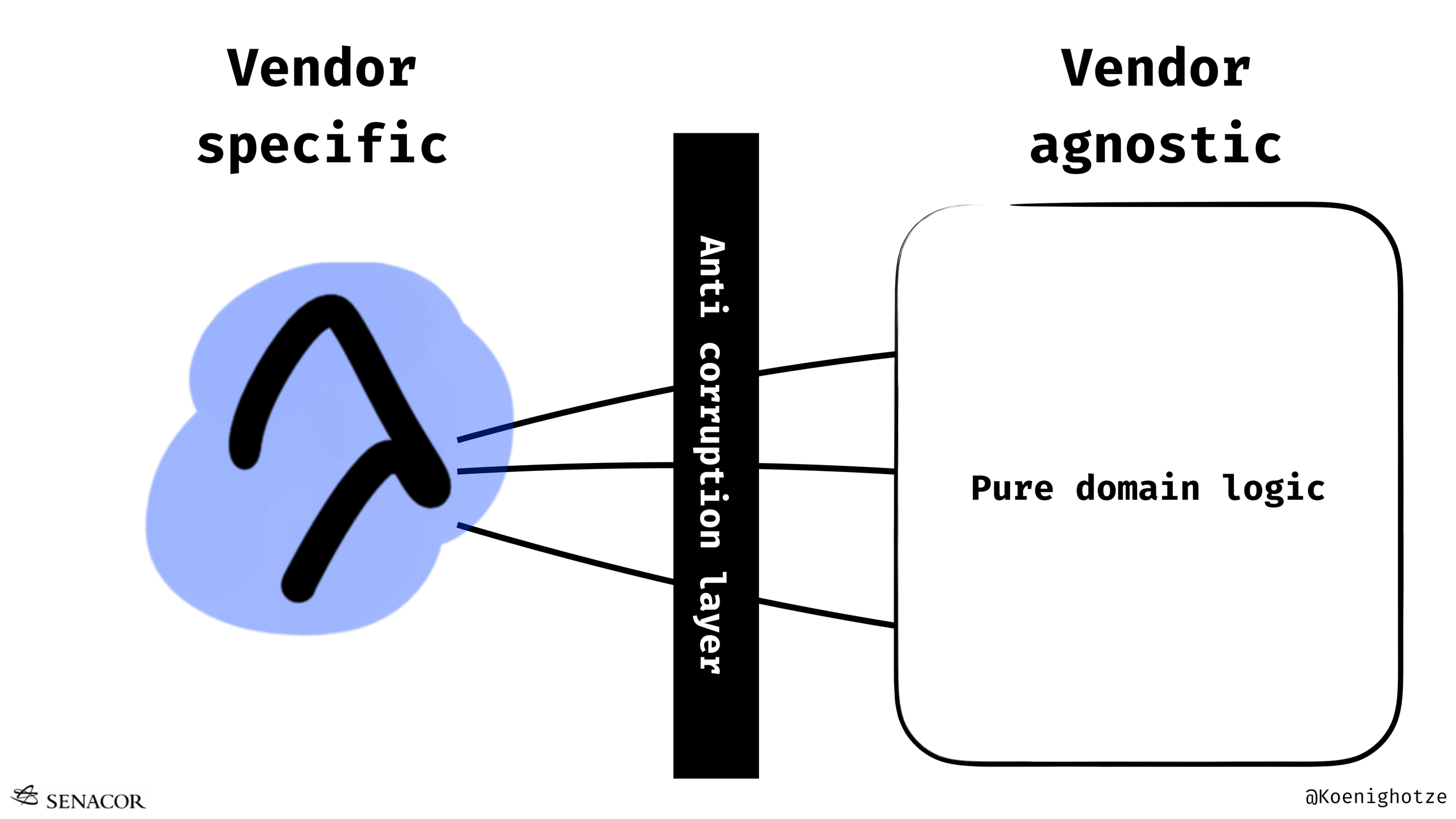
# COMMONS-LOGGING

# SEPARATE HANDLER AND BUSINESS CODE


Handler
create Order
forward Order
cancel Order


Handler
create Order
forward Order
cancel Order


Handler
Anti corruption layer
create Order
forward Order
cancel Order


Vendor specific
Vendor agnostic
Anti corruption layer
Pure domain logic

# YOU ABSOLUTELY NEED TOOLING FOR DEPLOYMENT

# AVOID UI DEPLOYMENTS

When you save your function with active tracing enabled, Lambda will automatically add permissions: "xray:PutTraceSegments", "xray:PutTelemetryRecords" to the function's current role if it does not have necessary permissions.

| Policy name |
| --- |
| AWSLambdaBasicExecutionRole-ef7… |
| AWSLambdaBasicExecutionRole-9ffe… |
| AWSLambdaBasicExecutionRole-7a4… |
| AWSLambdaBasicExecutionRole-76e… |
| AWSLambdaBasicExecutionRole-61a… |
| AWSLambdaBasicExecutionRole-19a… |

# AUTOMATION IS KEY

```
$ zip index.zip index.js node_modules
$ aws lambda create-function \
        --function-name HelloWorld \
        --runtime nodejs6.10 \
        --role arn:aws:iam::…:… \
        --handler index.handler \
        --zip-file fileb://index.zip
```

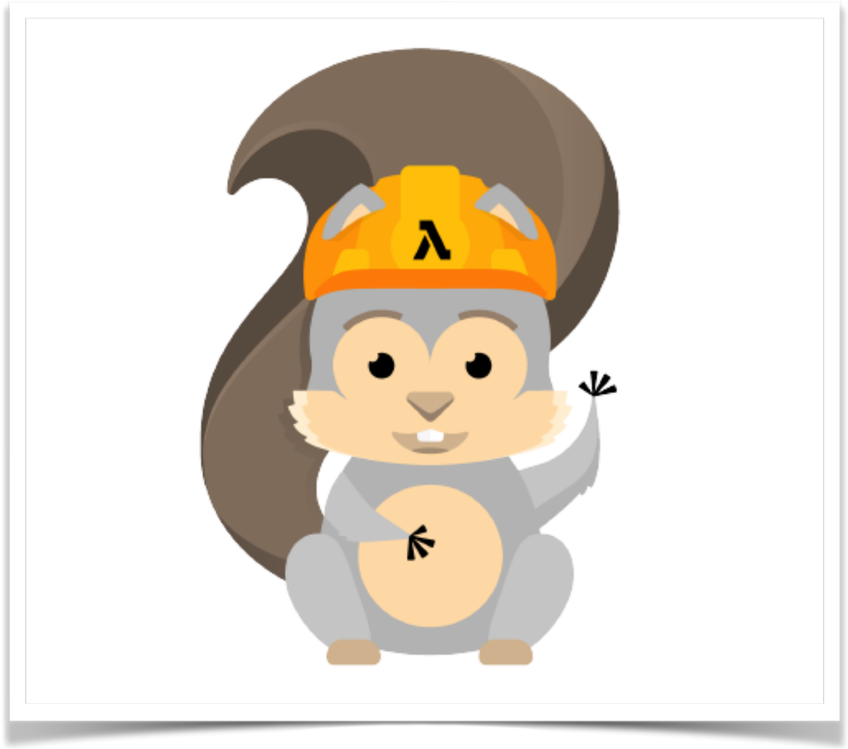
# TAGGING, UPDATE, RESOURCES, ROLES…


```
$ claudia create \
      --region eu-west-1 \
      --deploy-proxy-api \
      --handler index.handler \
      --name HelloWorld
```

# STATE, ROLLBACK, ERROR HANDLING…

# DECLARATIVE DEPLOYMENTS


Terraform



# AWS SERVERLESS APPLICATION MODEL

```yaml
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Description: Hello World
Resources:
  HelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Timeout: 5
      Runtime: nodejs6.10
      Handler: index.handler
      CodeUri: .
```

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Description: Hello World
Resources:
  HelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Timeout: 5
      Runtime: nodejs6.10
      Handler: index.handler
      CodeUri: .
```

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Description: Hello World
Resources:
  HelloWorld:
    Type: AWS::Serverless::Function
    Properties:
      Timeout: 5
      Runtime: nodejs6.10
      Handler: index.handler
      CodeUri: .
```

```
$ aws cloudformation package



$ aws cloudformation deploy
```

```
$ aws cloudformation package \
      --template-file sam.yaml \
      --s3-bucket somebucket   \
      > build/packaged.yaml
$ aws cloudformation deploy
```

```
$ aws cloudformation package \
      --template-file sam.yaml \
      --s3-bucket somebucket   \
      > build/packaged.yaml
$ aws cloudformation deploy
```

```
$ aws cloudformation package \
      --template-file sam.yaml \
      --s3-bucket somebucket   \
      > build/packaged.yaml
$ aws cloudformation deploy \
      --template-file build/packaged.yaml \
      --stack-name voxxed-demo  \
      --capabilities CAPABILITY_NAMED_IAM
```

```
$ aws cloudformation package \
      --template-file sam.yaml \
      --s3-bucket somebucket   \
      > build/packaged.yaml
$ aws cloudformation deploy \
      --template-file build/packaged.yaml \
      --stack-name voxxed-demo  \
      --capabilities CAPABILITY_NAMED_IAM
```

# ALL TOOLS HAVE

# DIFFERENT DRAWBACKS

# DEBUGGING

# DEBUGGING

# ROLLBACK

DEBUGGING

ROLLBACK

**STATE**

DEBUGGING

ROLLBACK

STATE

**FEATURE COMPLETENESS**


CLEANLINESS IS NEXT
TO GODLINESS


Netflix / SimianArmy
Code
Issues 27
Pull requests 5
Wiki
Releases
Janitor Home
Cory Bennett edited this page on Jan 5, 2015 · 7 revisions
What is Janitor Monkey?

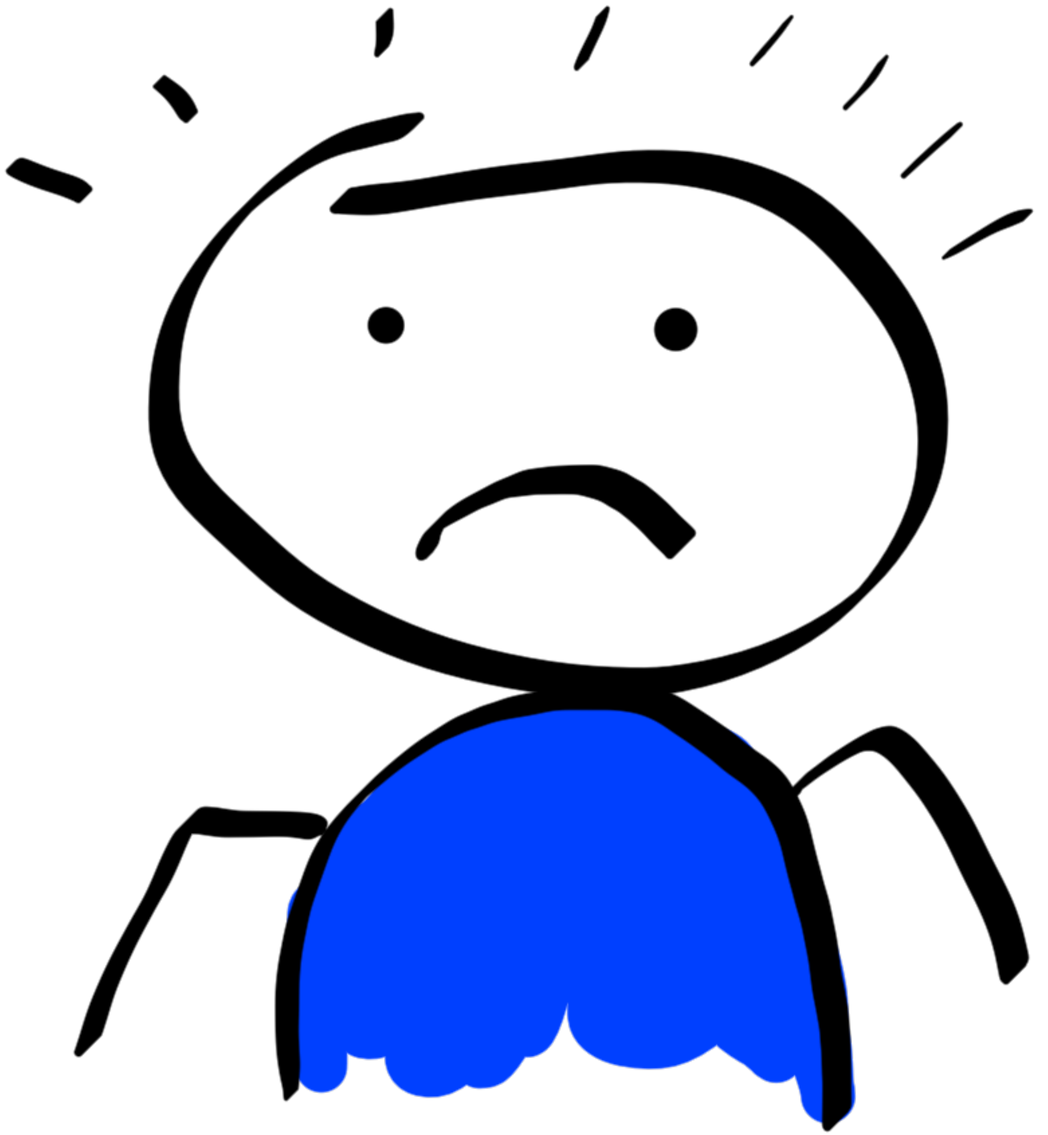
# TEST, TEST, TEST

# INTEGRATION TEST

# RIGHT FROM THE START


# SAM LOCAL

```
$ sam -version
sam version 0.2.6
```

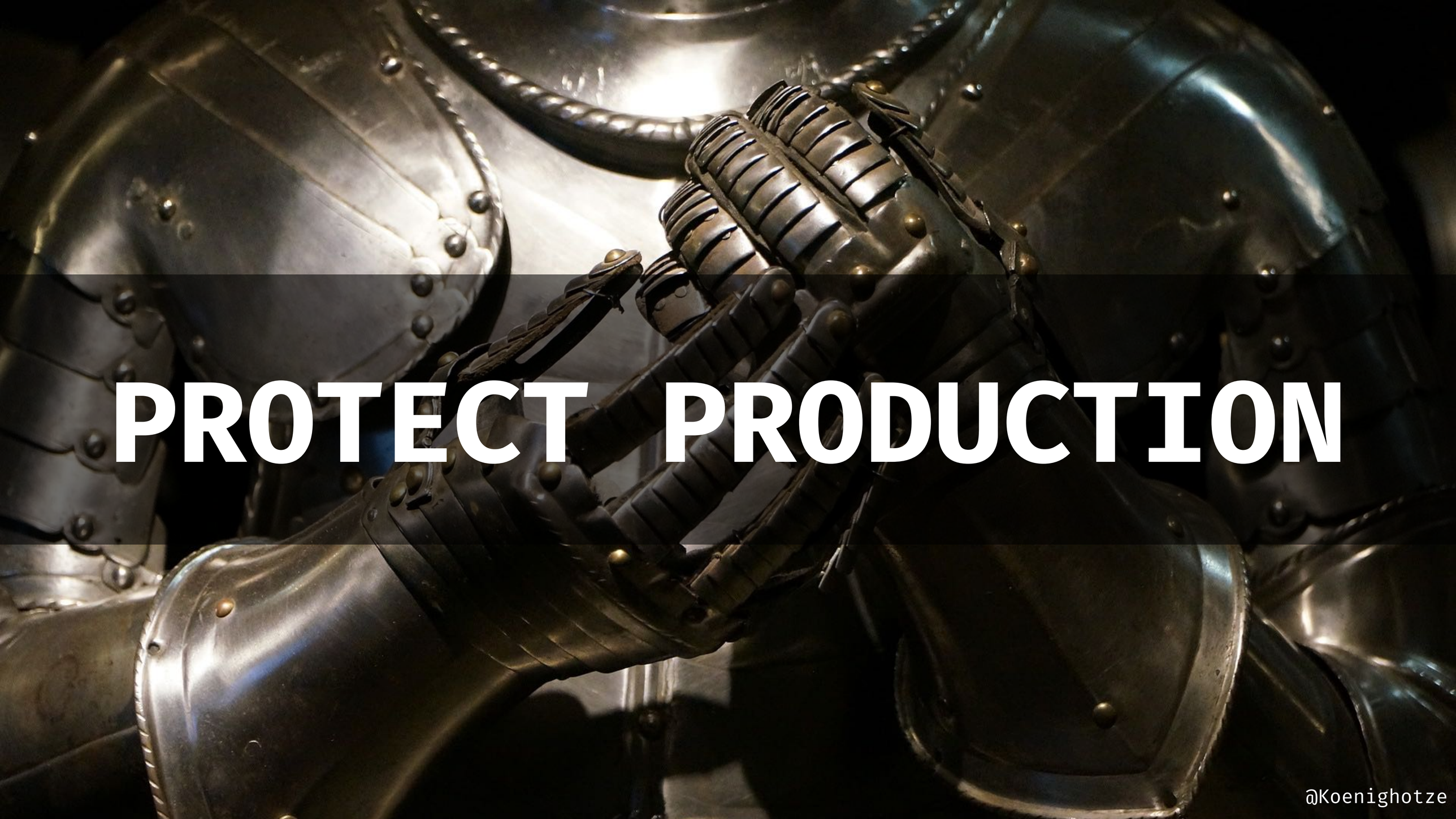


YOUR TESTING TOOLS SHOULD BE AS MATURE AS YOUR PRODUCTION TOOLS

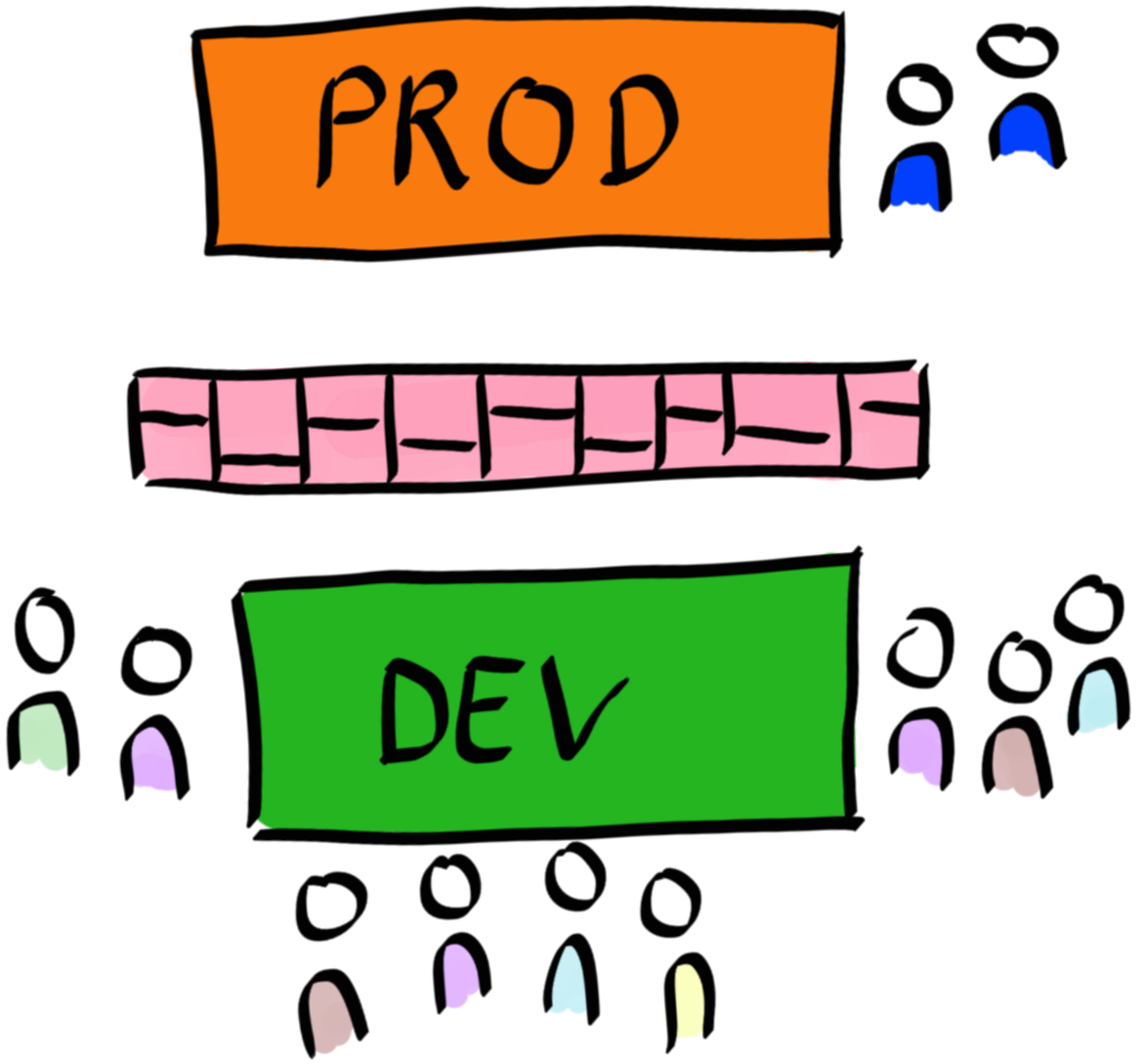
# TESTING LAMBDA FOR REAL IS JUST TOO EASY

```
aws lambda invoke \
    --function-name ReceiptUpload \
    --region eu-central-1 \
    --payload file://expensive_receipt.json \
    out.json
```

```
aws lambda invoke \
    --function-name ReceiptUpload \
    --region eu-central-1 \
    --payload file://expensive_receipt.json \
    out.json
```


PROTECT PRODUCTION
@Koenighotze

# STAGING IS A THING


PROD
DEV

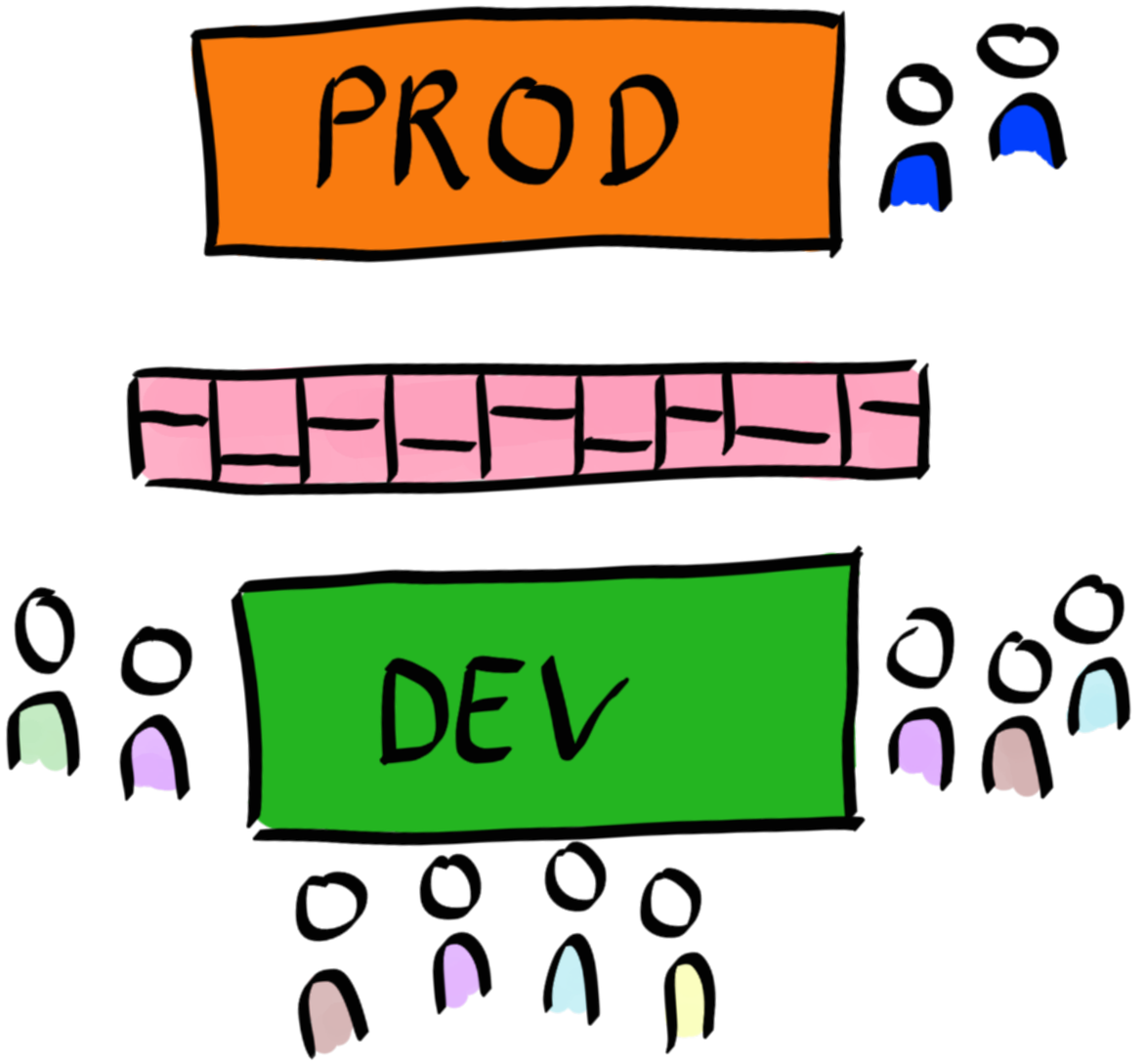
```
Parameters:
    …
    Stage:
      Type: String
      Default: DEV

ForwardBilling:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: !Sub ForwardBilling-${Stage}
```

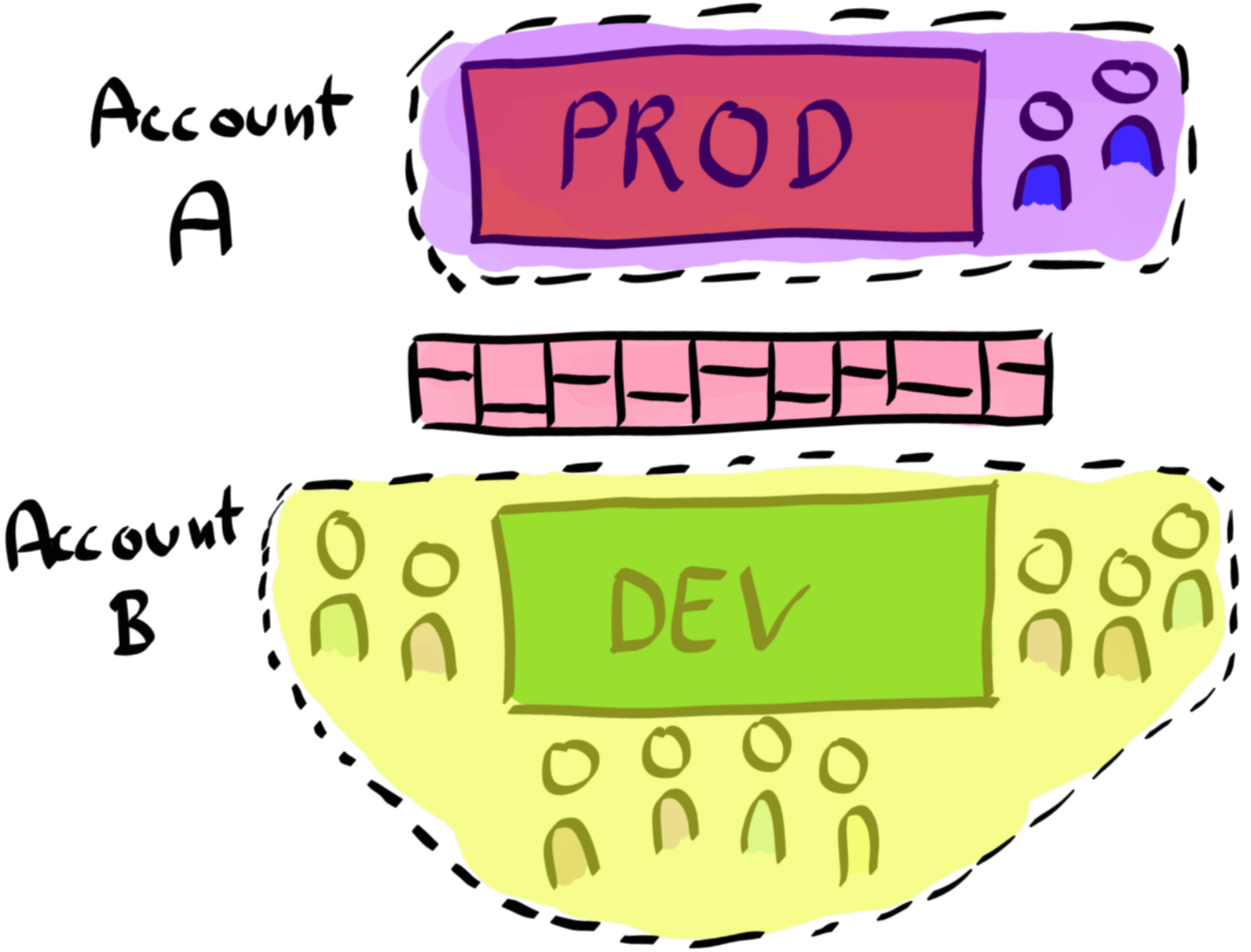
```
Parameters:
    …
    Stage:
      Type: String
      Default: DEV

ForwardBilling:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: !Sub ForwardBilling-${Stage}
```

```
aws cloudformation deploy
      --template-file …
      --stack-name …
      --parameter-overrides Stage=PROD
```

```
aws cloudformation deploy
      --template-file …
      --stack-name …
      --parameter-overrides Stage=PROD
```

# PROTECT STAGES WITH ACCOUNTS


PROD
DEV


Account
A
PROD
Account
B
DEV

```
aws cloudformation deploy
      …
      --parameter-overrides Stage=PROD
      --profile ACCOUNT_A
```

```
aws cloudformation deploy
      …
      --parameter-overrides Stage=PROD
      --profile ACCOUNT_A
```

# CLEANUP UNUSED LAMBDAS


@Koenighotze

# HOW DO YOU REASON ABOUT CLOUD ARCHITECTURES?

# HOW TO KNOW WHAT TO CLEANUP?

https://github.com/epsagon/list-lambdas

```
PYTHON LIST_LAMBDAS.PY \
       –INACTIVE-DAYS-FILTER 10
```

| Region | Function | Last Modified | Last Invocation |
|---|---|---|---|
| eu-central-1 | digital_logistics_03_fb_webhook | 54 days ago | 42 days ago |
| eu-central-1 | fis-projects-dev-newProject | 53 days ago | 54 days ago |
| eu-central-1 | marlon_login_handler | 54 days ago | 54 days ago |
| eu-central-1 | copy-picture-lambda-dev-hello | 144 days ago | 144 days ago |
| eu-central-1 | Fis2_0-Contract-DismissContract | 52 days ago | 52 days ago |
| eu-central-1 | marlon_account_linking | 54 days ago | 54 days ago |
| eu-central-1 | test | 238 days ago | 238 days ago |
| eu-central-1 | digital_logistics_03_user_login | 55 days ago | 42 days ago |
| eu-central-1 | fis-projects-dev-getProjects | 53 days ago | 52 days ago |
| eu-central-1 | Fis2_0-Employees-GetEmployees | 53 days ago | 27 days ago |
| eu-central-1 | digital_logistics_03_dialogflow_webhook | 55 days ago | 39 days ago |
| eu-central-1 | transactions-api-dev-getpictures | 144 days ago | 143 days ago |
| eu-central-1 | digital_logistics_03_update_parcel_status | 55 days ago | 42 days ago |
| eu-central-1 | LambdaHelloWorldTest | 144 days ago | N/A (no invocations?) |
| eu-central-1 | AwsWatchDog | 7 days ago | 7 days ago |
| eu-central-1 | Fis2_0-Contract-GetContractByEmployee | 52 days ago | 27 days ago |
| eu-central-1 | fis-projects-dev-deleteProject | 53 days ago | 54 days ago |
| eu-central-1 | HelloWorld | 88 days ago | 88 days ago |
| eu-central-1 | Fis2_0-Employees-GetEmployee | 53 days ago | 53 days ago |
| eu-central-1 | Fis2_0-Employees-GetContractByEmployee | 53 days ago | 53 days ago |
| eu-central-1 | fis-projects-dev-getProject | 53 days ago | 54 days ago |
| eu-west-1 | digital_logistics_alexa_handler | 55 days ago | 55 days ago |
| eu-west-1 | theMotivator | 111 days ago | 72 days ago |
| eu-west-1 | DevconScheduleToSpeech | 97 days ago | 94 days ago |
| eu-west-1 | wasserstandinfo | 36 days ago | 8 days ago |

| Region | Function | Last Modified | Last Invocation |
|---|---|---|---|
| eu-central-1 | fis-projects-dev-newProject | 53 days ago | 54 days ago |
| eu-central-1 | marlon_login_handler | 54 days ago | 54 days ago |
| eu-central-1 | copy-picture-lambda-dev-hello | 144 days ago | 144 days ago |
| eu-central-1 | Fis2_0-Contract-DismissContract | 52 days ago | 52 days ago |
| eu-central-1 | marlon_account_linking | 54 days ago | 54 days ago |
| eu-central-1 | test | 238 days ago | 238 days ago |
| eu-central-1 | digital_logistics_03_user_login | 55 days ago | 42 days ago |
| eu-central-1 | fis-projects-dev-getProjects | 53 days ago | 52 days ago |
| eu-central-1 | Fis2_0-Employees-GetEmployees | 53 days ago | 27 days ago |
| eu-central-1 | digital_logistics_03_dialogflow_webhook | 55 days ago | 39 days ago |
| eu-central-1 | transactions-api-dev-getpictures | 144 days ago | 143 days ago |
| eu-central-1 | digital_logistics_03_update_parcel_status | 55 days ago | 42 days ago |
| eu-central-1 | LambdaHelloWorldTest | 144 days ago | N/A (no invocations?) |
| eu-central-1 | AwsWatchDog | 7 days ago | 7 days ago |
| eu-central-1 | Fis2_0-Contract-GetContractByEmployee | 52 days ago | 27 days ago |
| eu-central-1 | fis-projects-dev-deleteProject | 53 days ago | 54 days ago |
| eu-central-1 | HelloWorld | 88 days ago | 88 days ago |
| eu-central-1 | Fis2_0-Employees-GetEmployee | 53 days ago | 53 days ago |
| eu-central-1 | Fis2_0-Employees-GetContractByEmployee | 53 days ago | 53 days ago |
| eu-central-1 | fis-projects-dev-getProject | 53 days ago | 54 days ago |
| eu-west-1 | digital_logistics_alexa_handler | 55 days ago | 55 days ago |
| eu-west-1 | theMotivator | 111 days ago | 72 days ago |
| eu-west-1 | DevconScheduleToSpeech | 97 days ago | 94 days ago |
| eu-west-1 | wasserstandinfo | 36 days ago | 8 days ago |

| Region | Function | Last Modified | Last Invocation |
|---|---|---|---|
| eu-central-1 | digital_logistics_03_fb_webhook | 54 days ago | 42 days ago |
| eu-central-1 | fis-projects-dev-newProject | 53 days ago | 54 days ago |
| eu-central-1 | marlon_login_handler | 54 days ago | 54 days ago |
| eu-central-1 | copy-picture-lambda-dev-hello | 144 days ago | 144 days ago |
| eu-central-1 | Fis2_0-Contract-DismissContract | 52 days ago | 52 days ago |
| eu-central-1 | test | 238 days ago | 238 days ago |
| eu-central-1 | fis-projects-dev-getProjects | 53 days ago | 52 days ago |
| eu-central-1 | Fis2_0-Employees-GetEmployees | 53 days ago | 27 days ago |
| eu-central-1 | digital_logistics_03_dialogflow_webhook | 55 days ago | 39 days ago |
| eu-central-1 | transactions-api-dev-getpictures | 144 days ago | 143 days ago |
| eu-central-1 | digital_logistics_03_update_parcel_status | 55 days ago | 42 days ago |
| eu-central-1 | LambdaHelloWorldTest | 144 days ago | N/A (no invocations?) |
| eu-central-1 | AwsWatchDog | 7 days ago | 7 days ago |
| eu-central-1 | Fis2_0-Contract-GetContractByEmployee | 52 days ago | 27 days ago |
| eu-central-1 | fis-projects-dev-deleteProject | 53 days ago | 54 days ago |
| eu-central-1 | HelloWorld | 88 days ago | 88 days ago |
| eu-central-1 | Fis2_0-Employees-GetEmployee | 53 days ago | 53 days ago |
| eu-central-1 | Fis2_0-Employees-GetContractByEmployee | 53 days ago | 53 days ago |
| eu-central-1 | fis-projects-dev-getProject | 53 days ago | 54 days ago |
| eu-west-1 | digital_logistics_alexa_handler | 55 days ago | 55 days ago |
| eu-west-1 | theMotivator | 111 days ago | 72 days ago |
| eu-west-1 | DevconScheduleToSpeech | 97 days ago | 94 days ago |
| eu-west-1 | wasserstandinfo | 36 days ago | 8 days ago |

# REDUCE ATTACK SURFACE

REDUCE ATTACK SURFACE

REDUCE COGNITIVE

CLUTTER

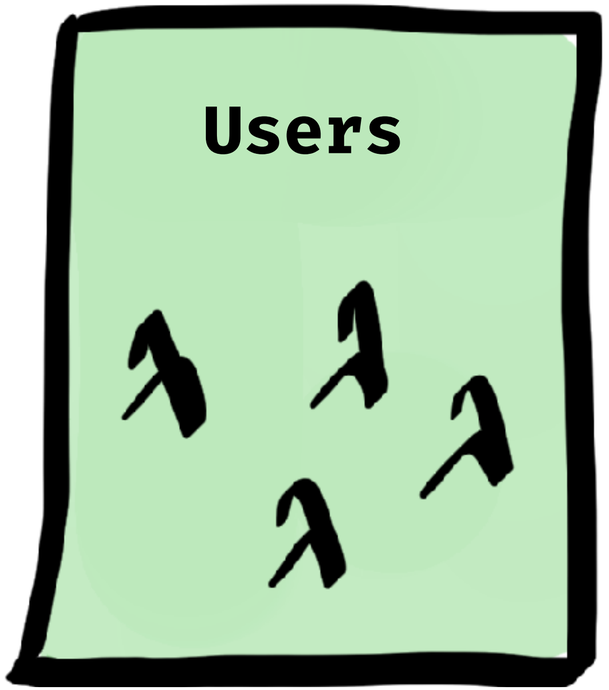
# REDUCE ATTACK SURFACE

# REDUCE COGNITIVE CLUTTER

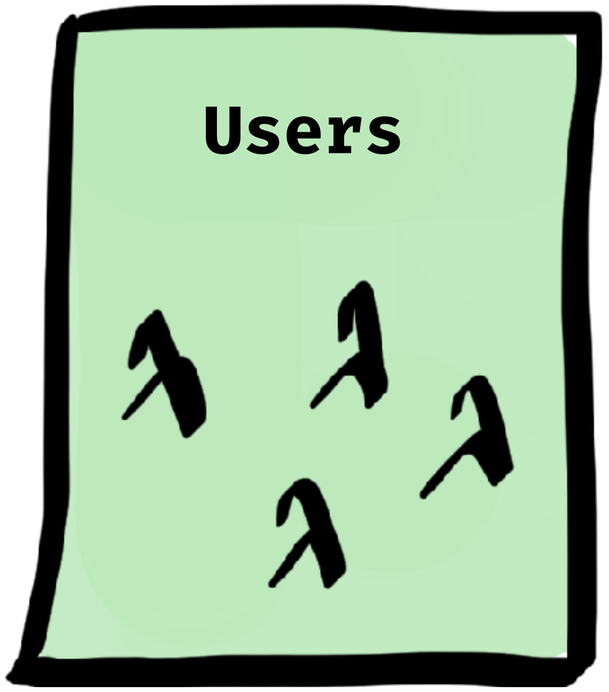
# STAY IN CONTROL


HOT AND COLD
@Koenighotze

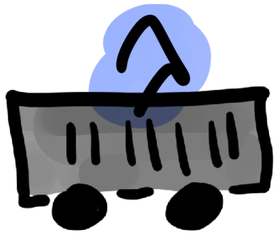
# COLD START HAPPENS ONCE, RIGHT?

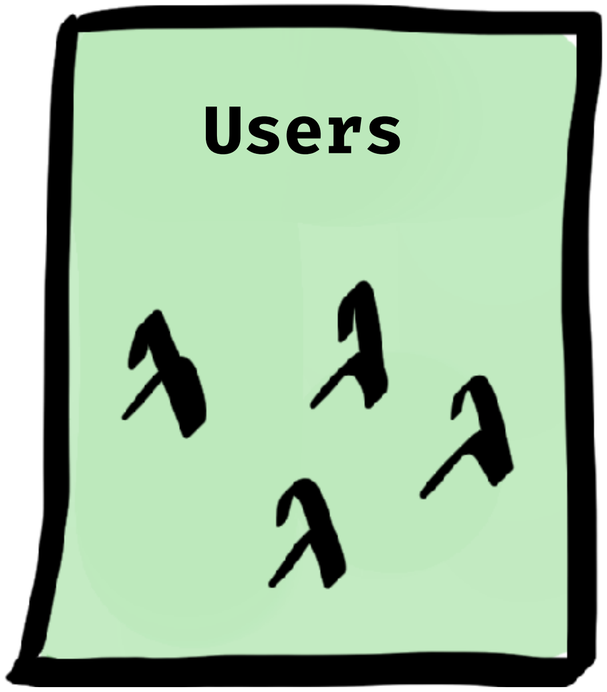

Users


Event

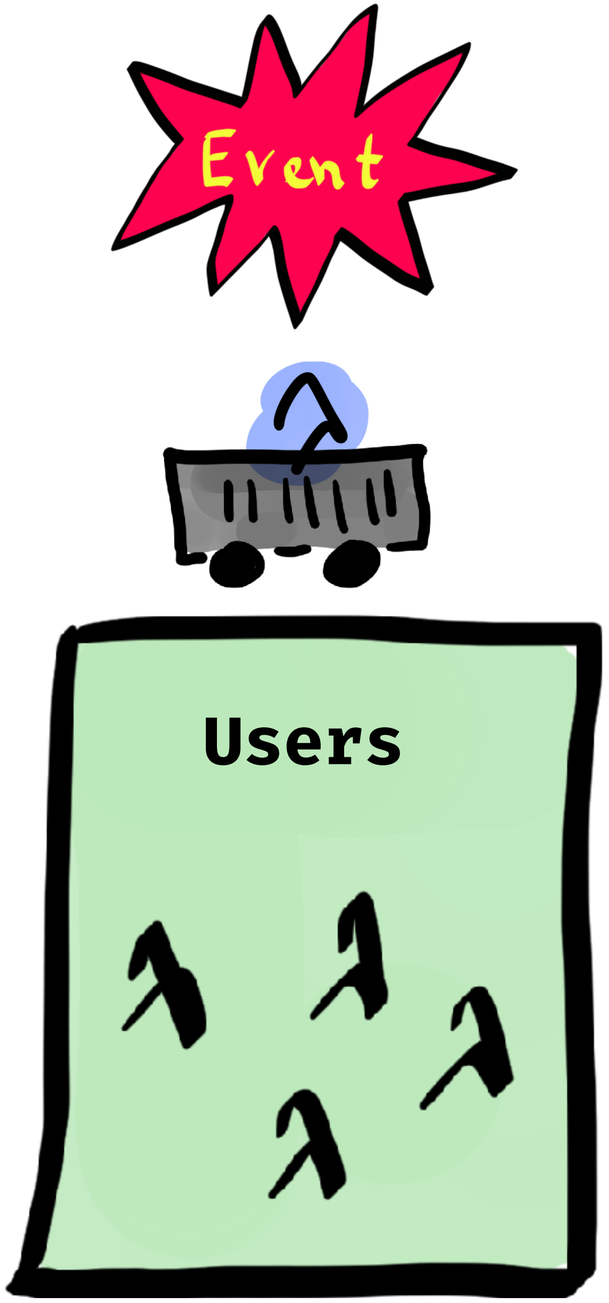

Users


## Cold

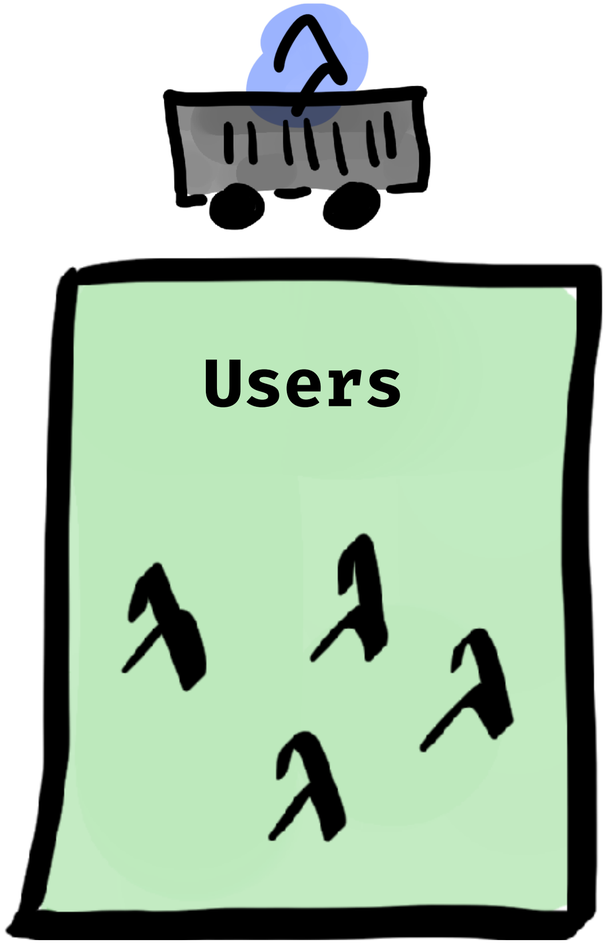




Cold



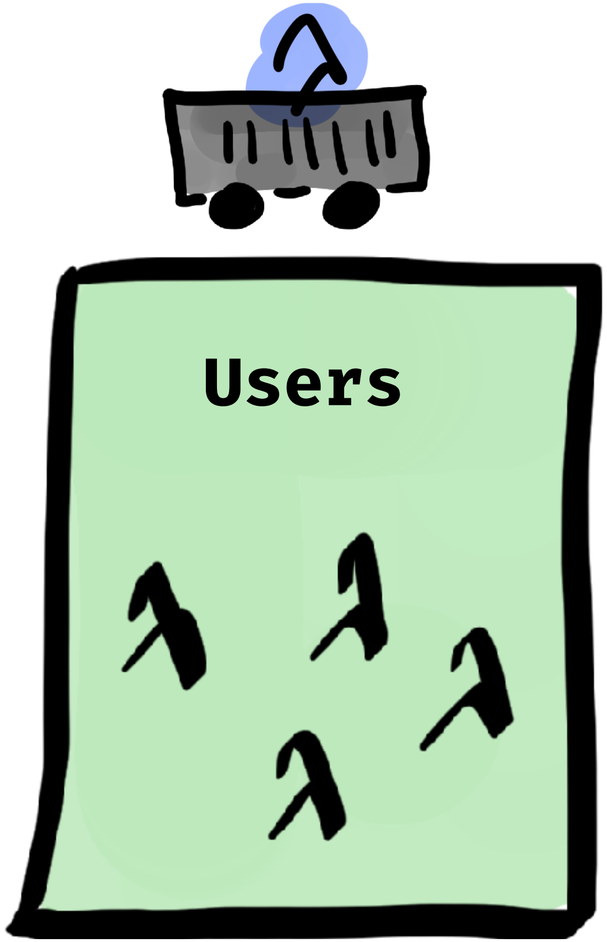
Cold



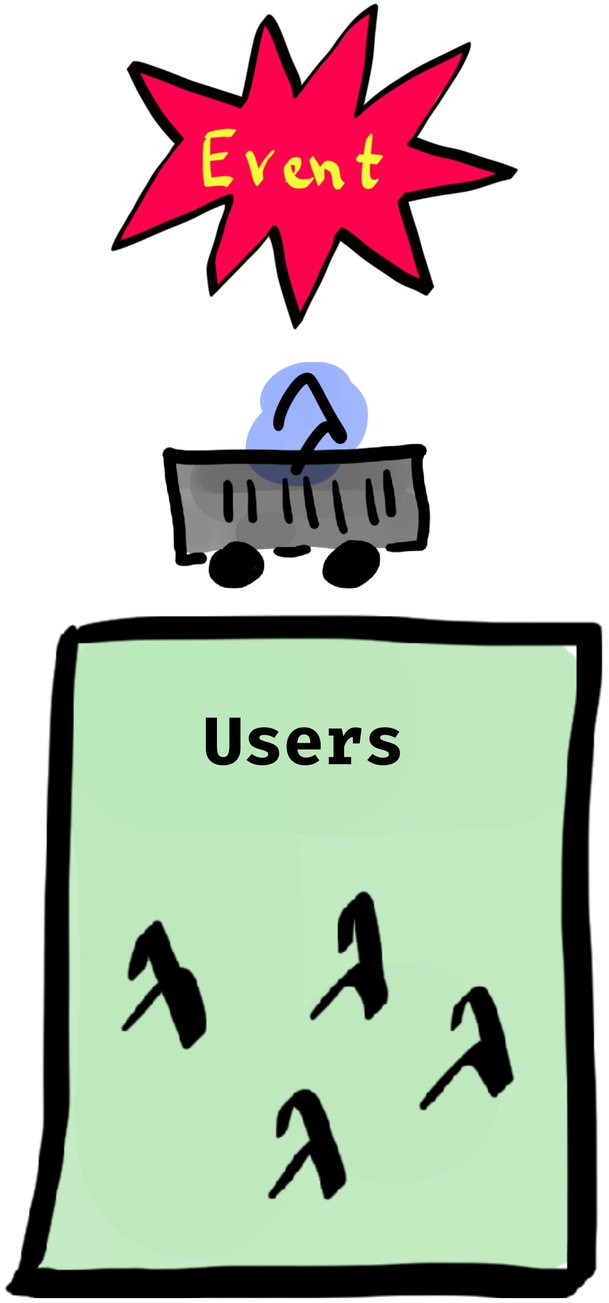

# COLD

# START

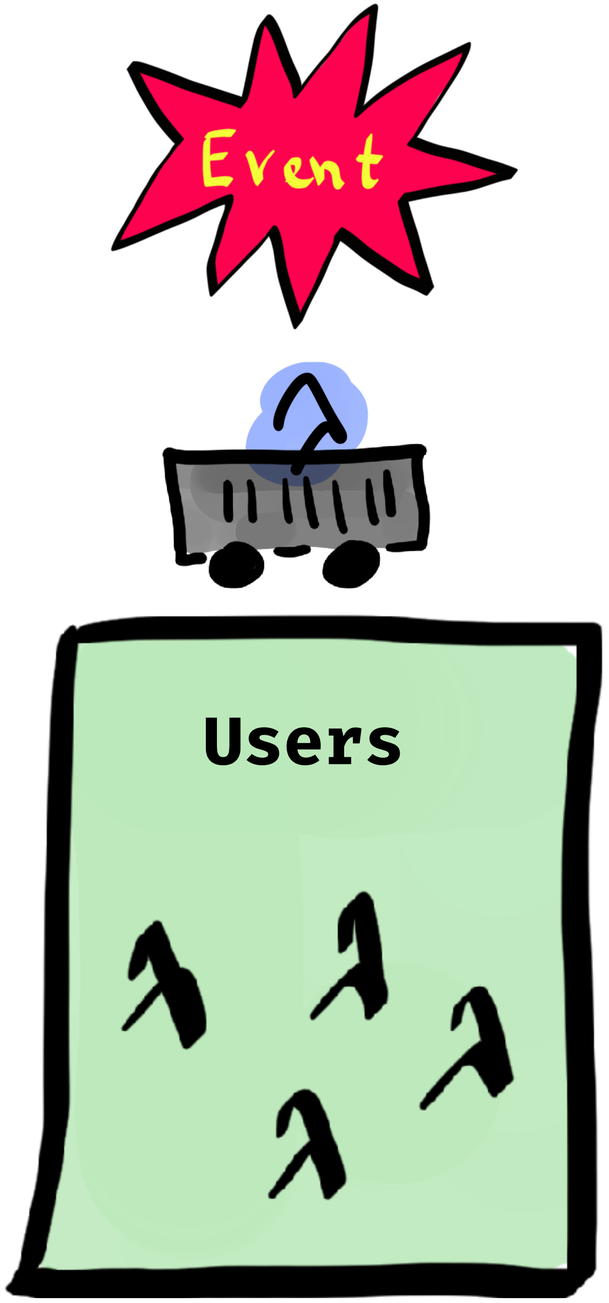
Cold



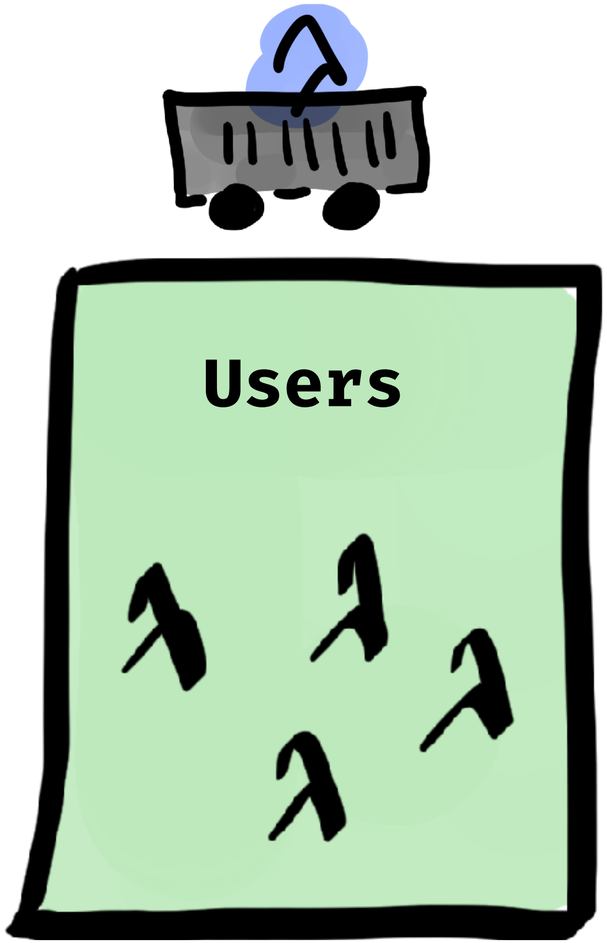
Cold



Cold



Cold

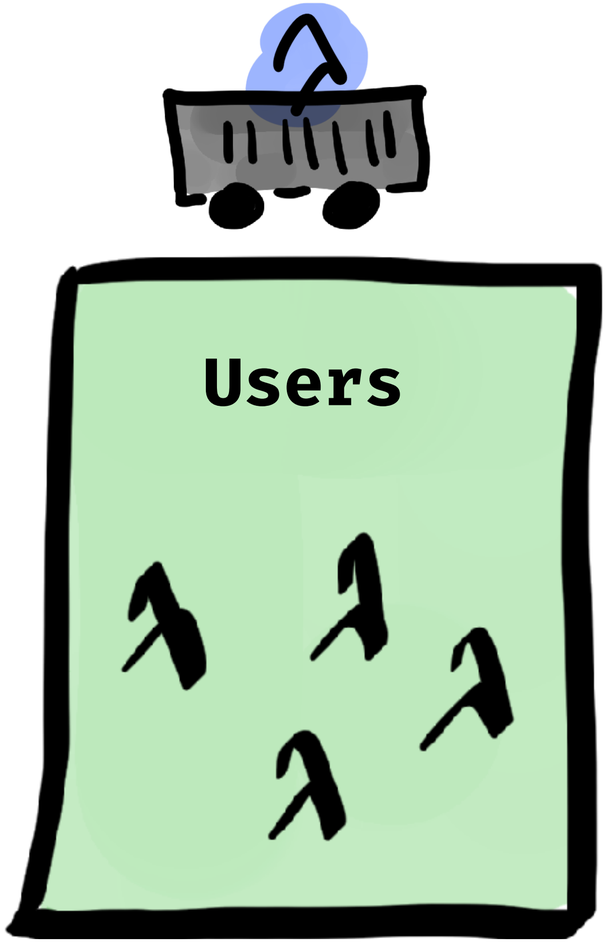



HOT

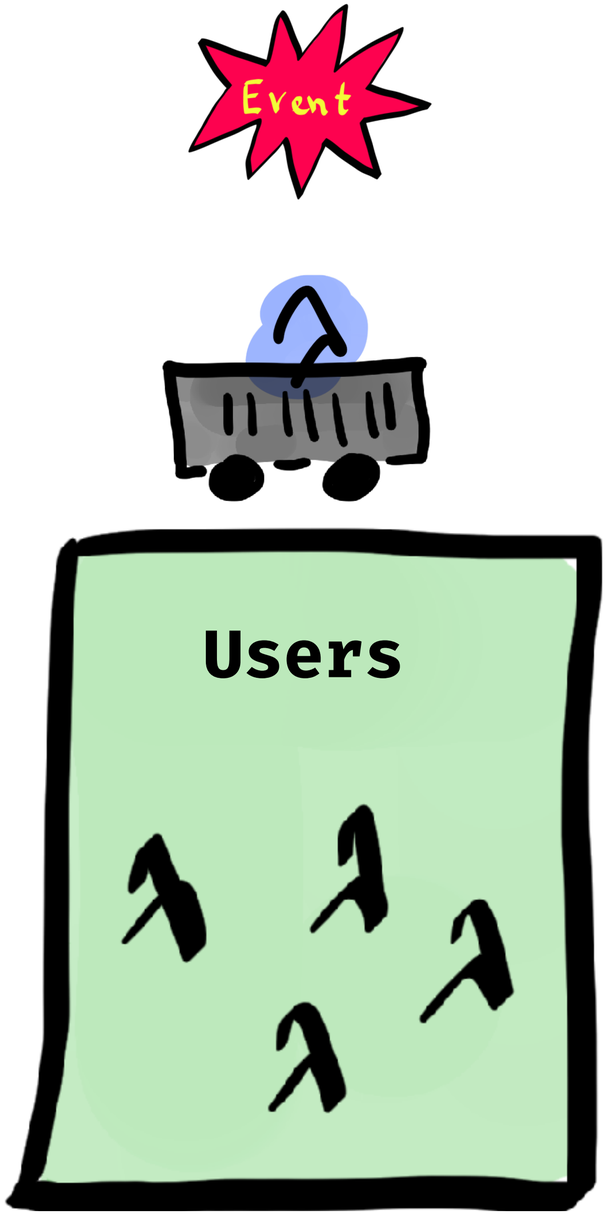
START

# SCALE BY REQUEST

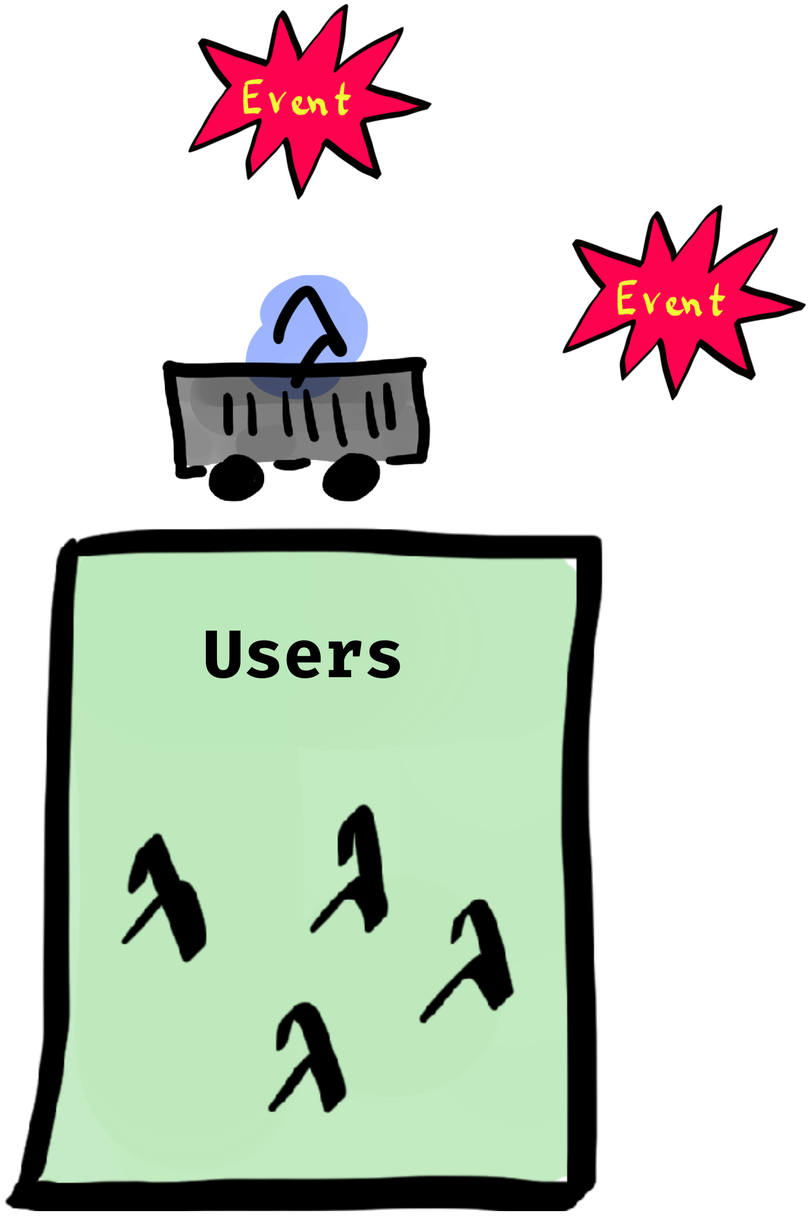
Cold



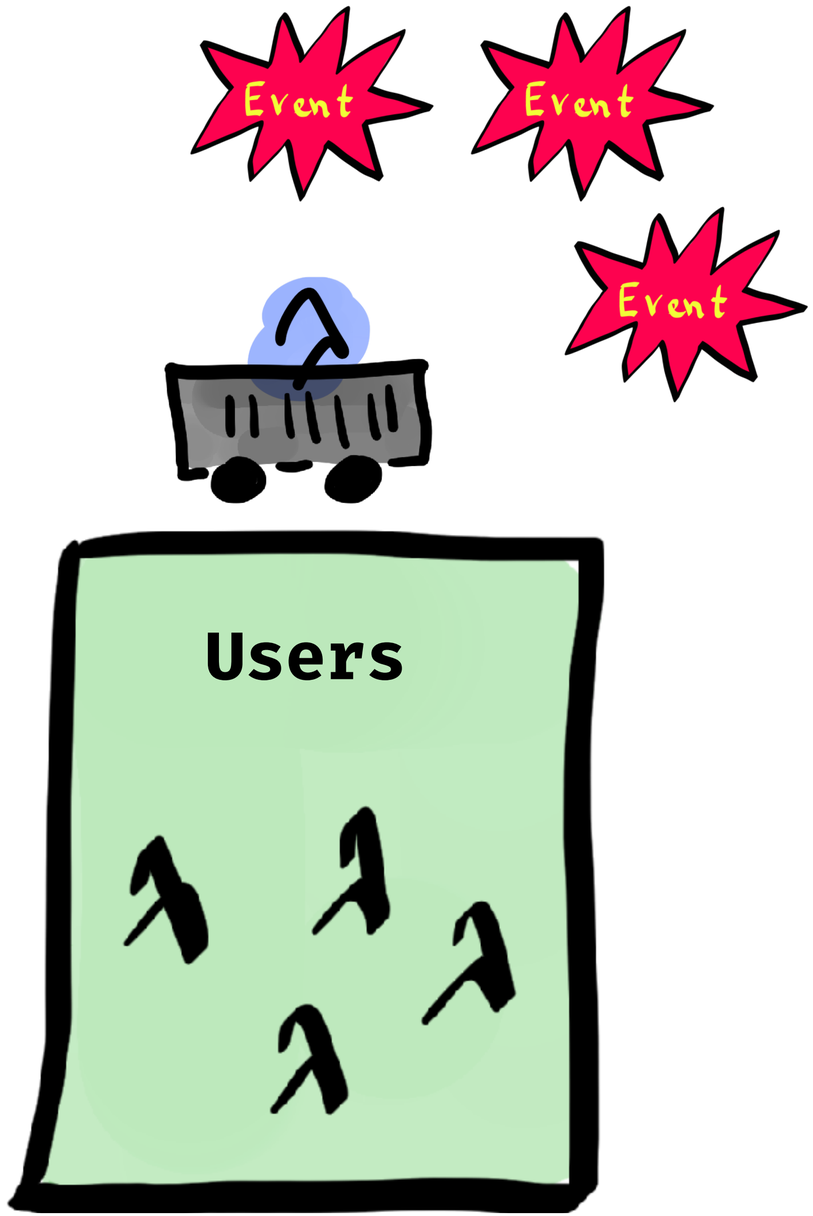
Cold



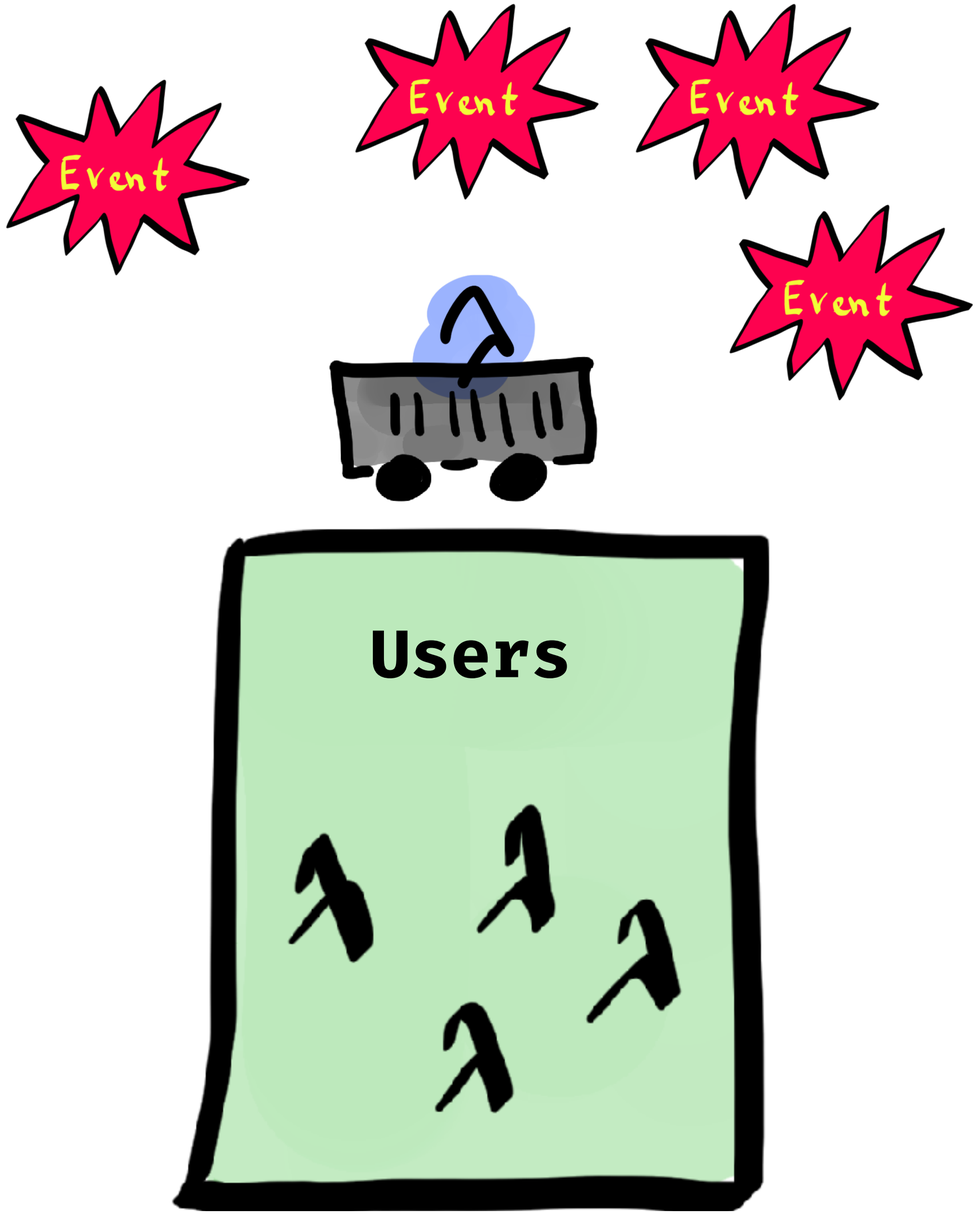
# Cold



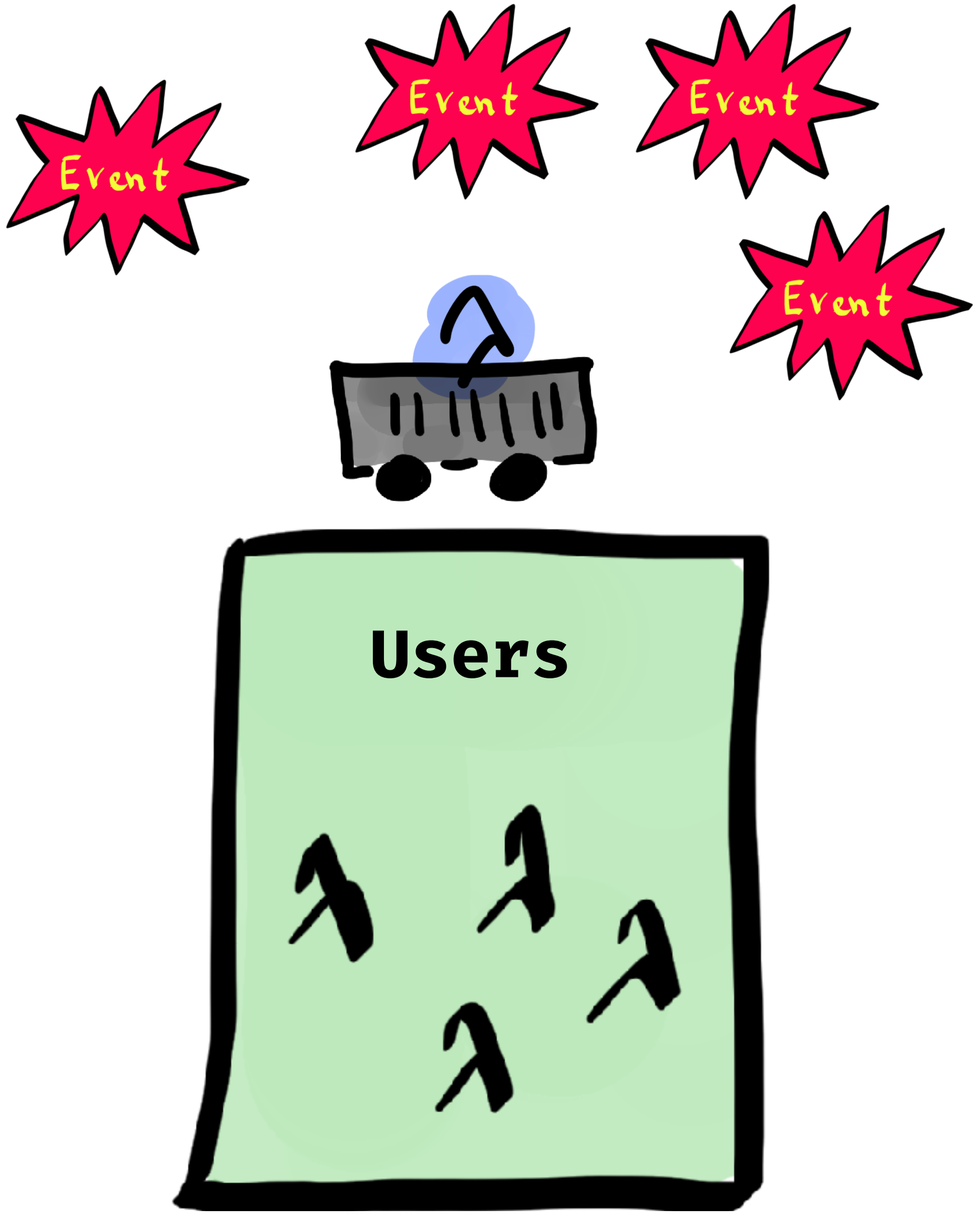
Cold



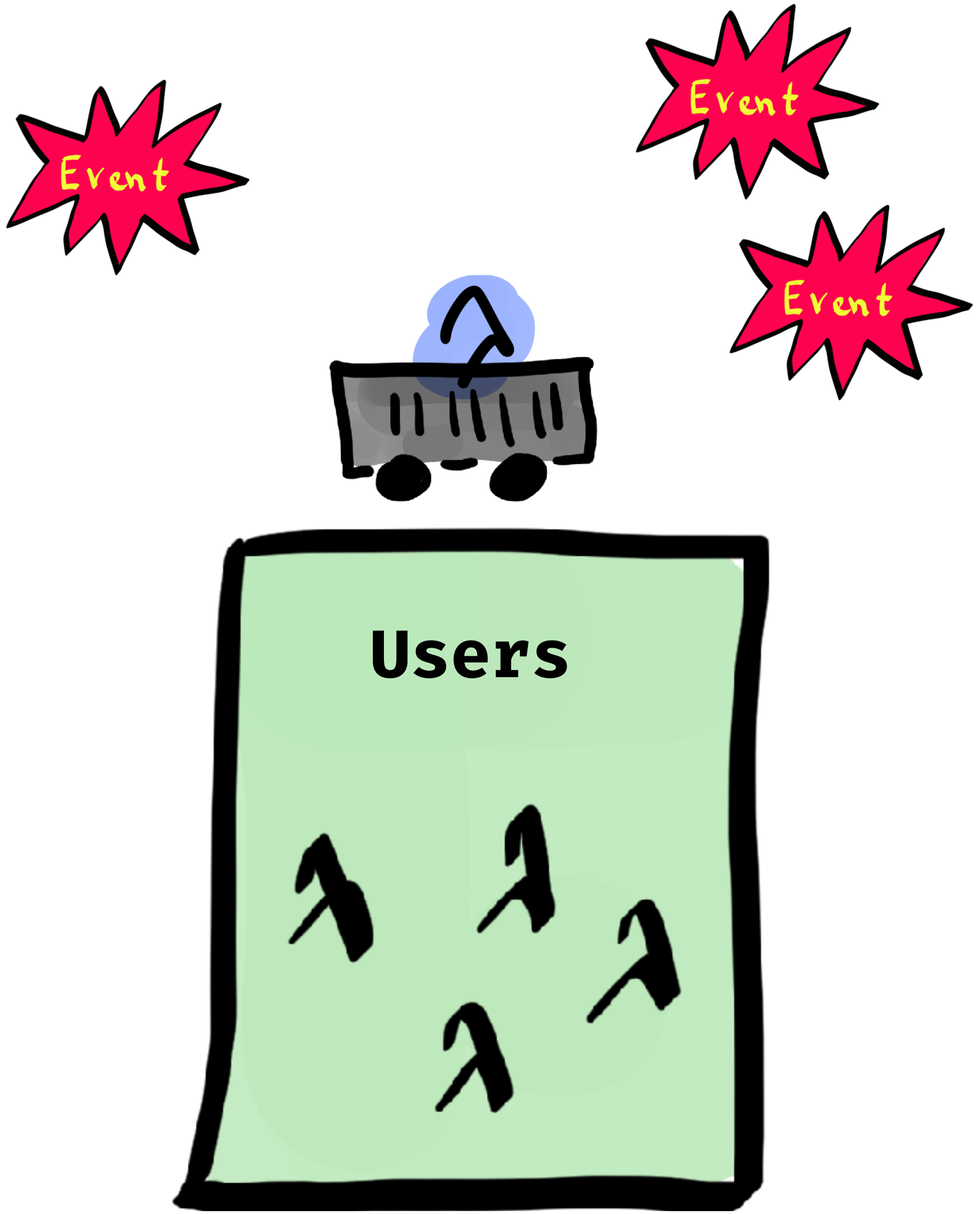
# Cold

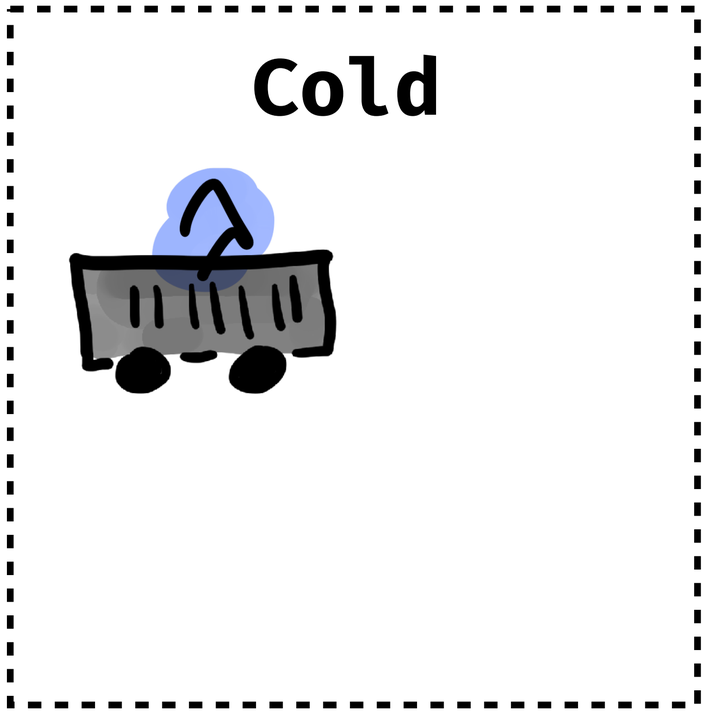


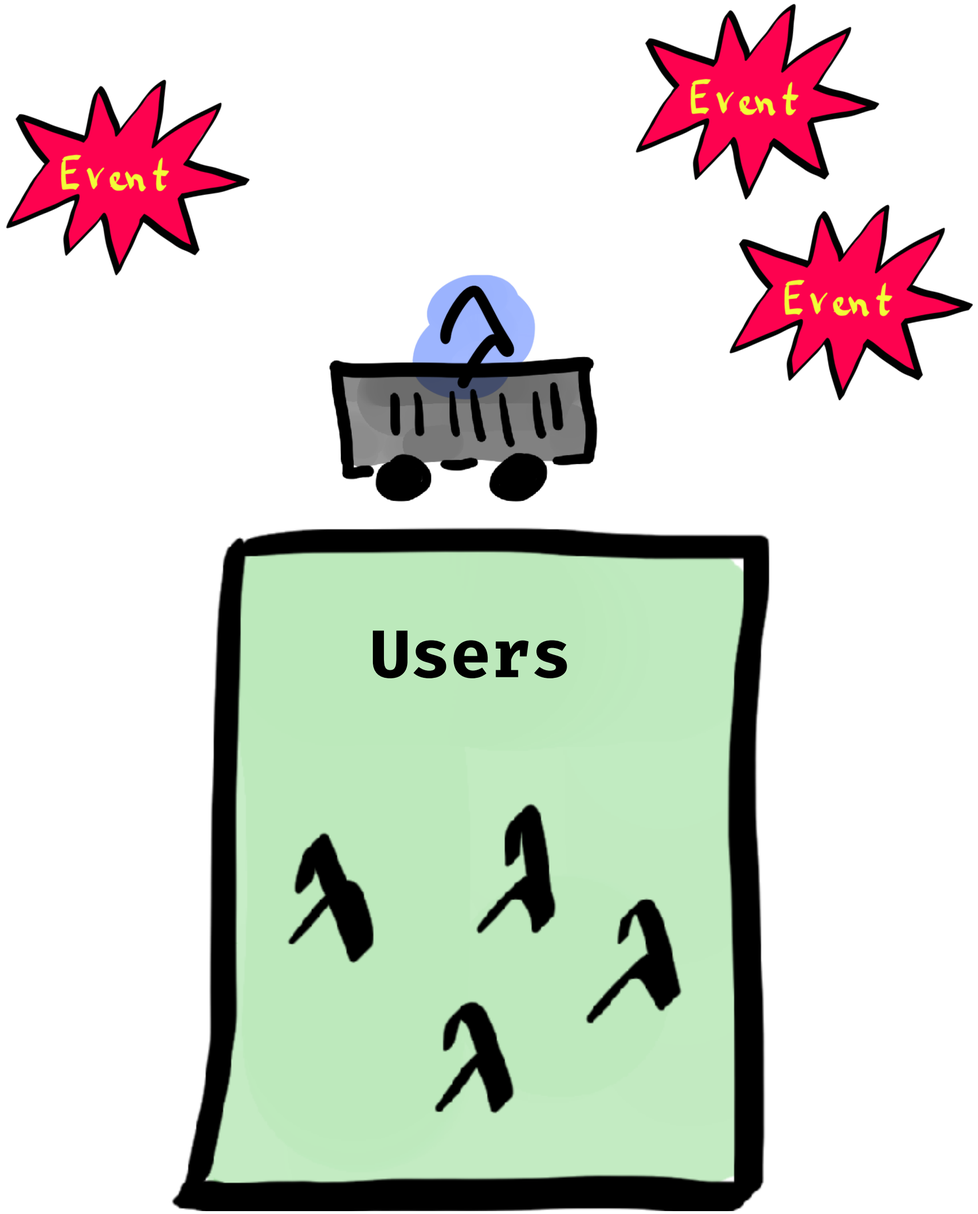
# Cold



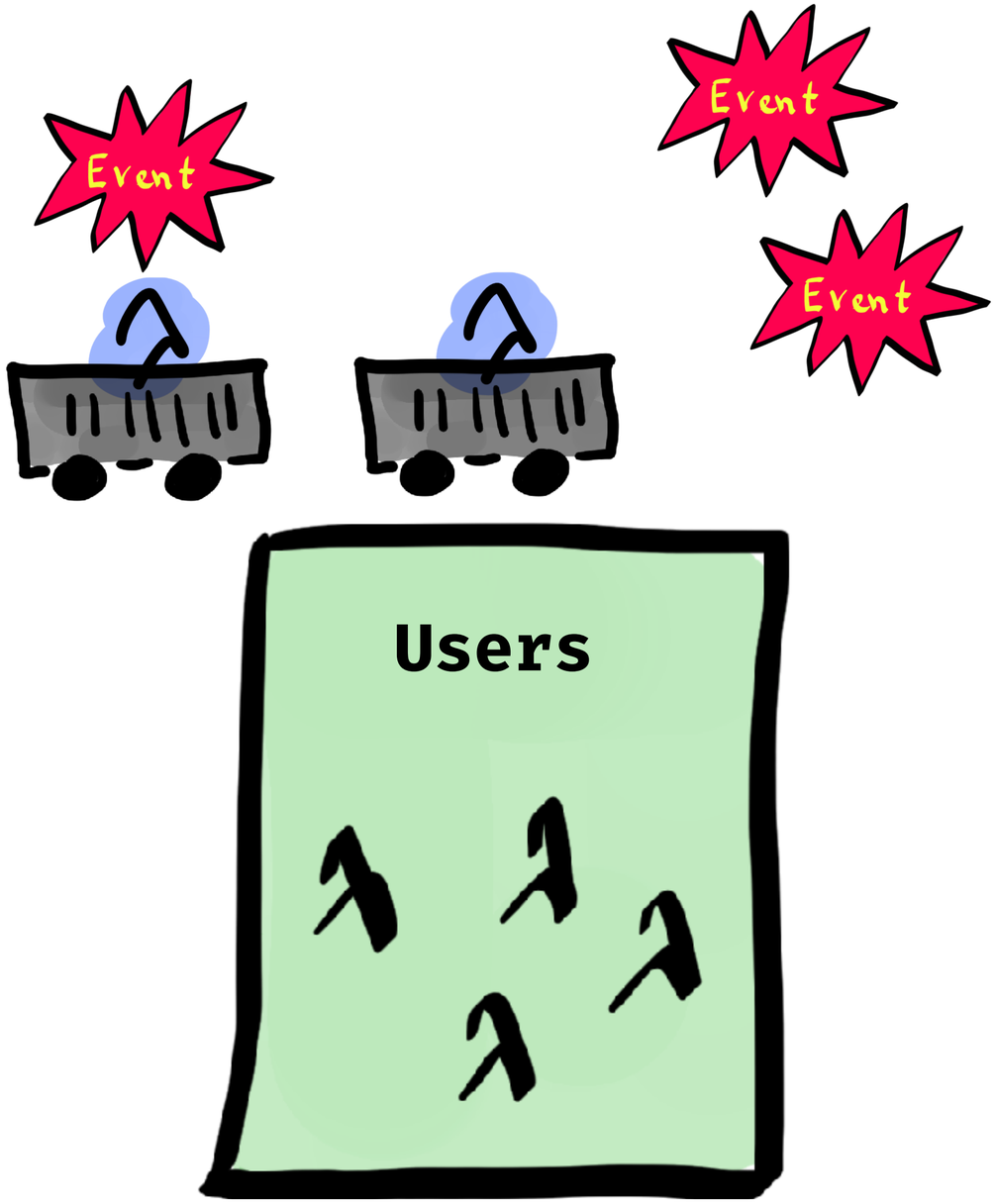
Cold

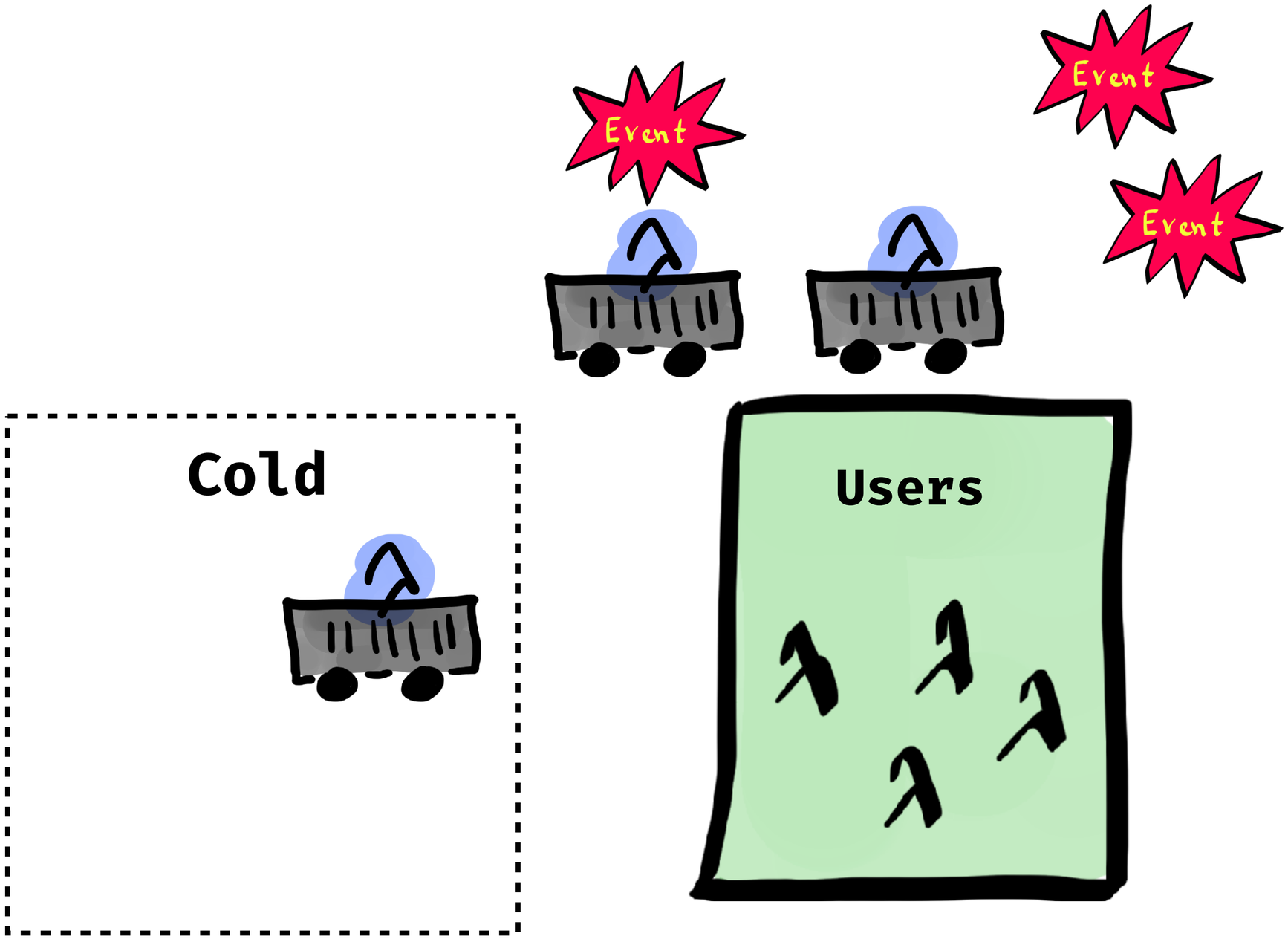



Cold

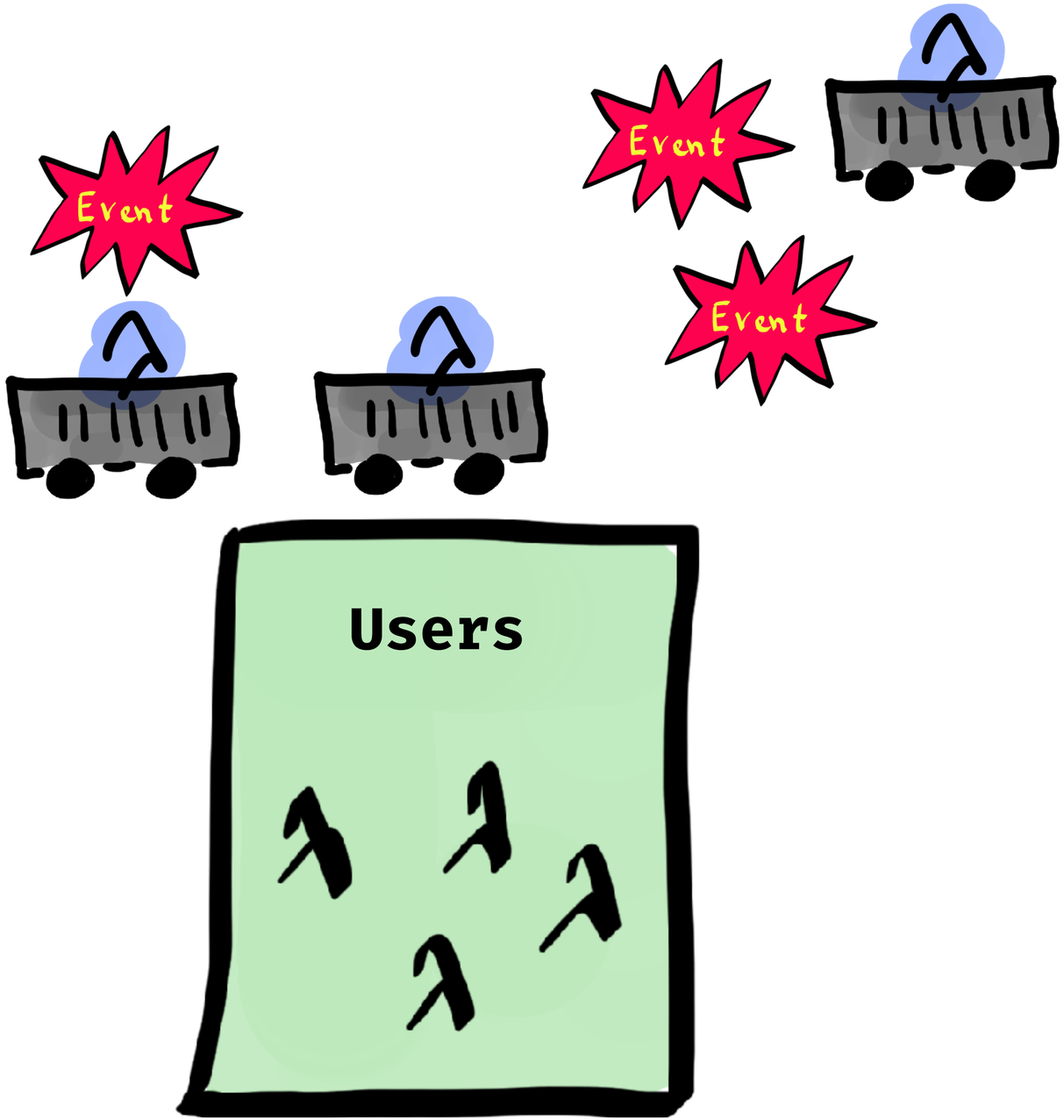

Event
Event
Event
Users

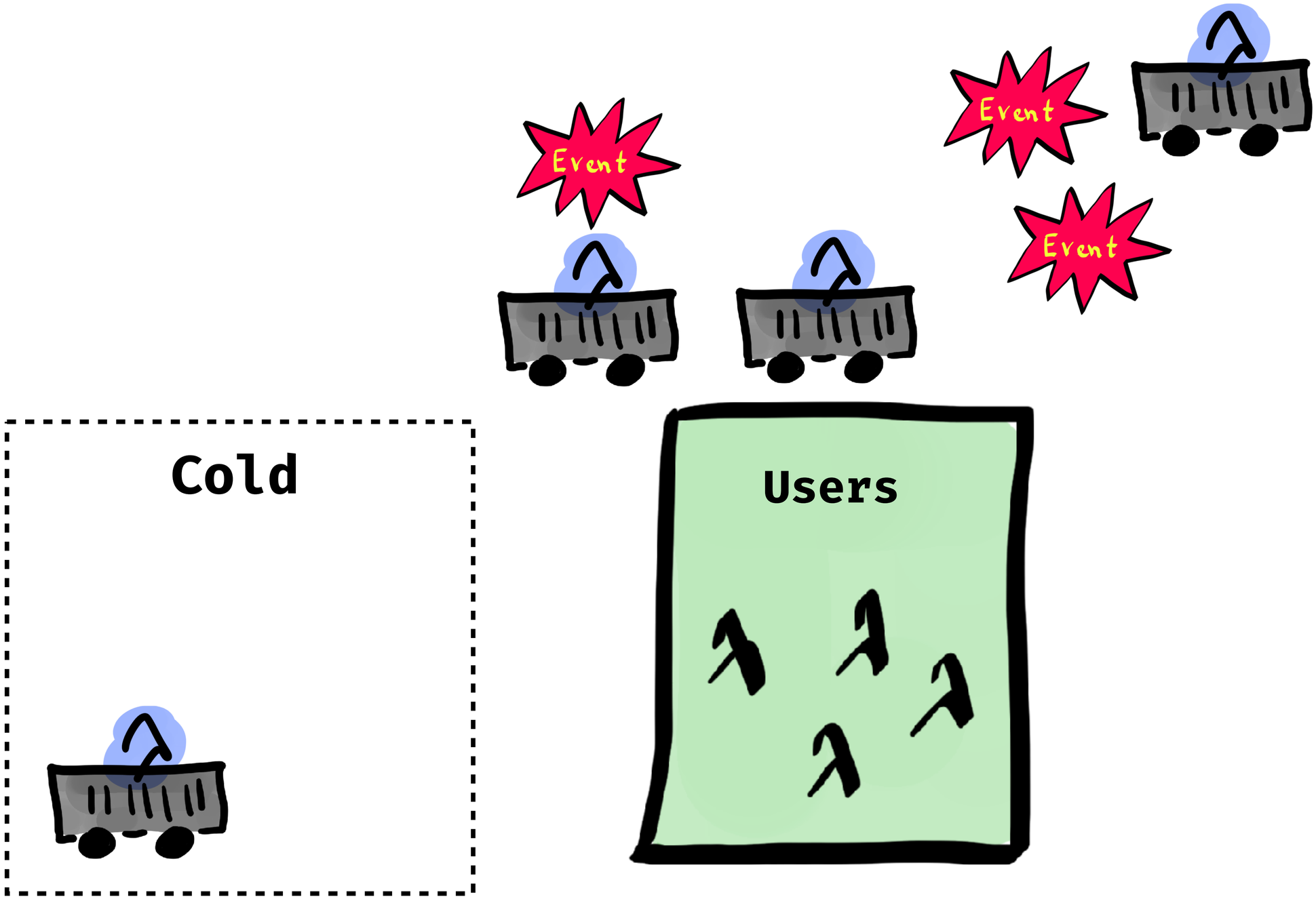
# Cold



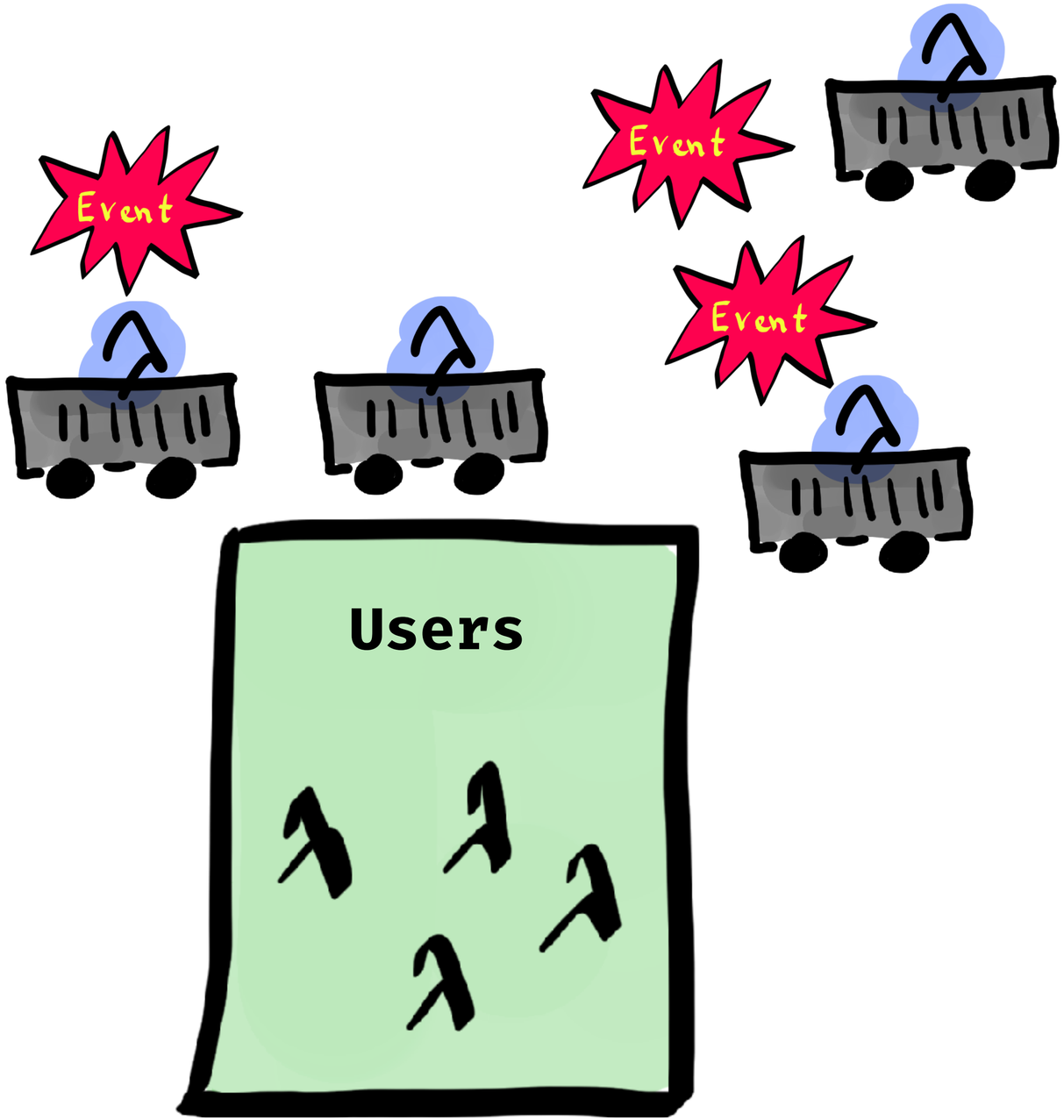

Event
Event
Event
Users
Cold

# Cold

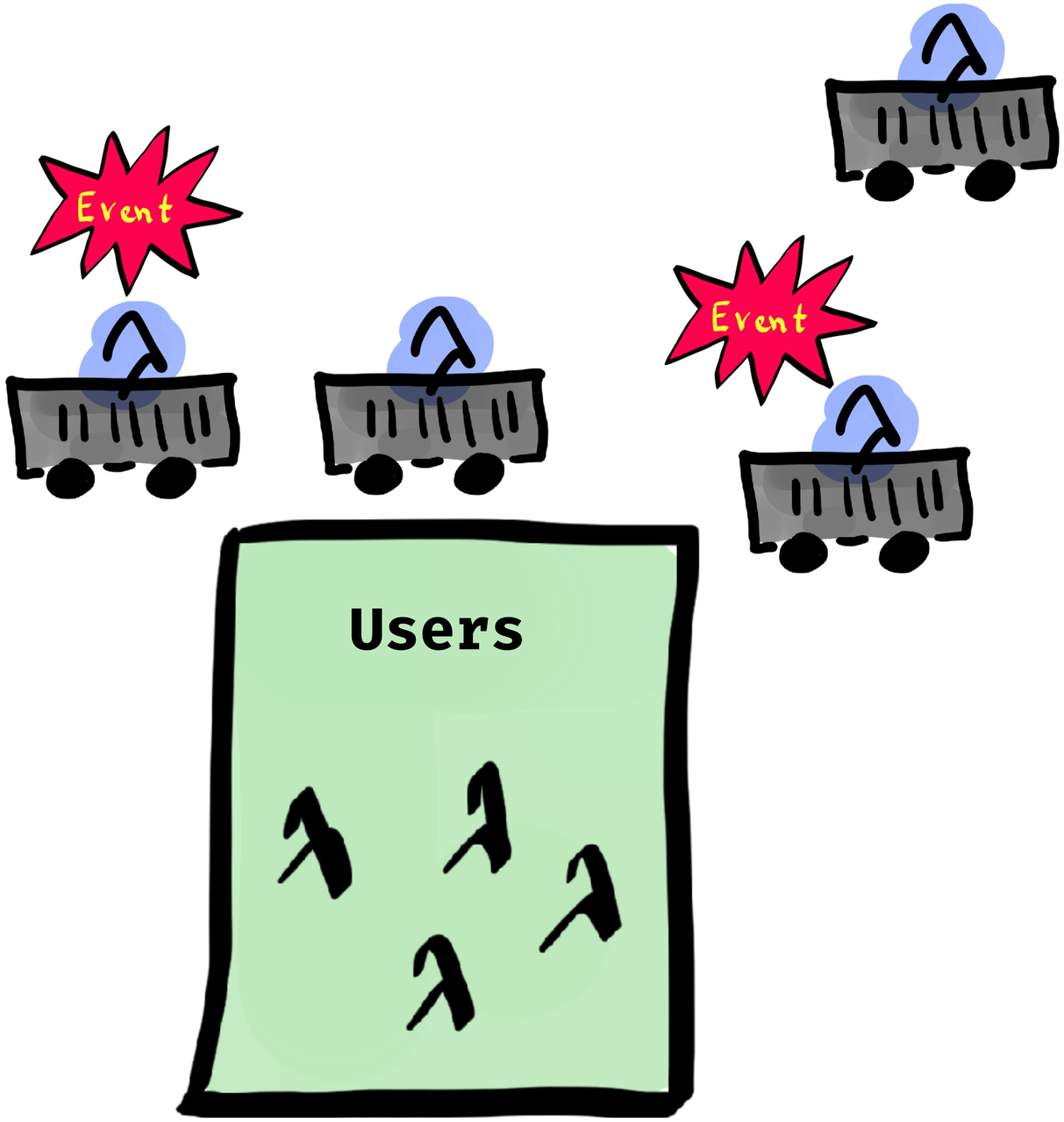



Event
Event
Event
Cold
Users

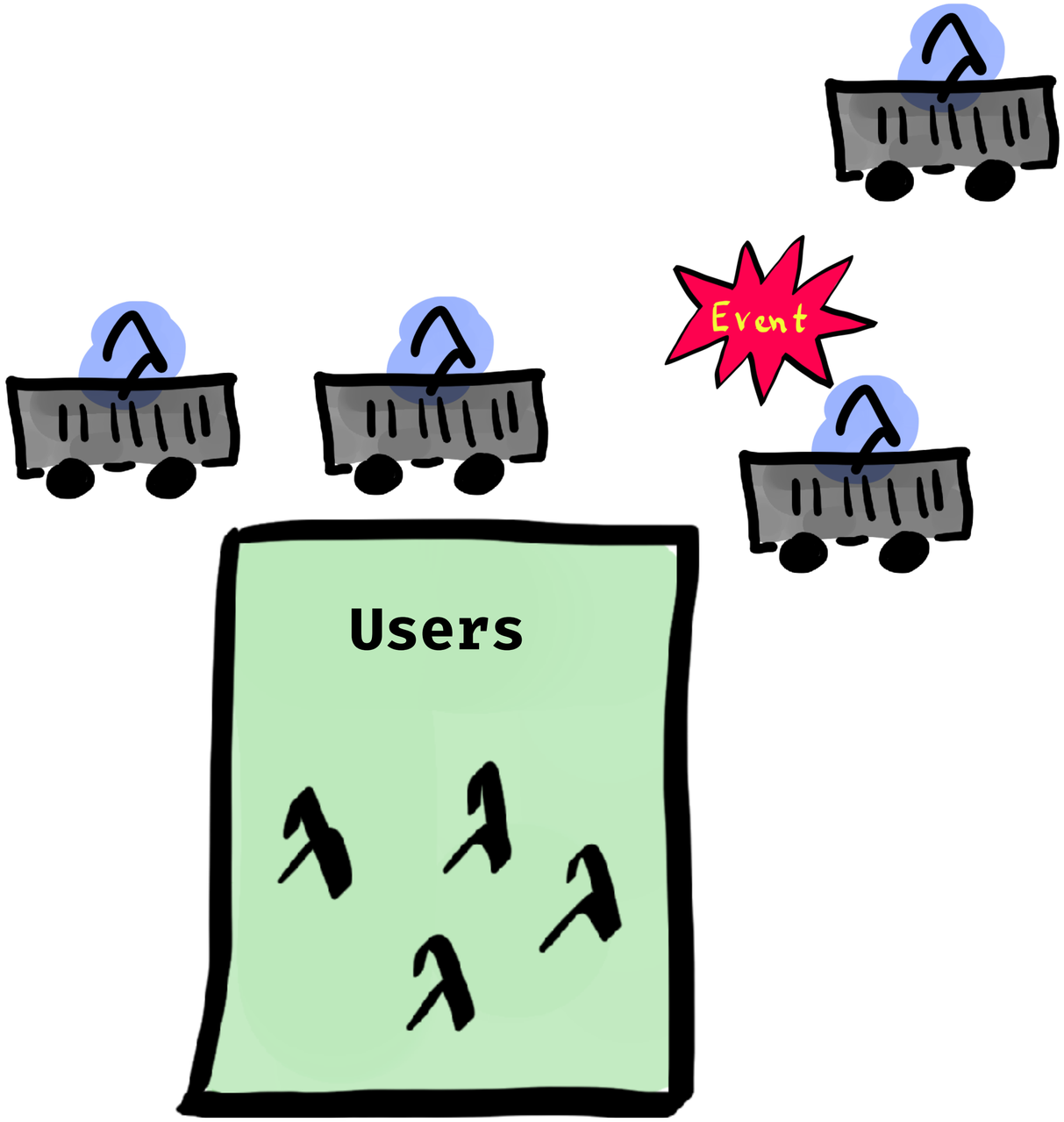
# Cold



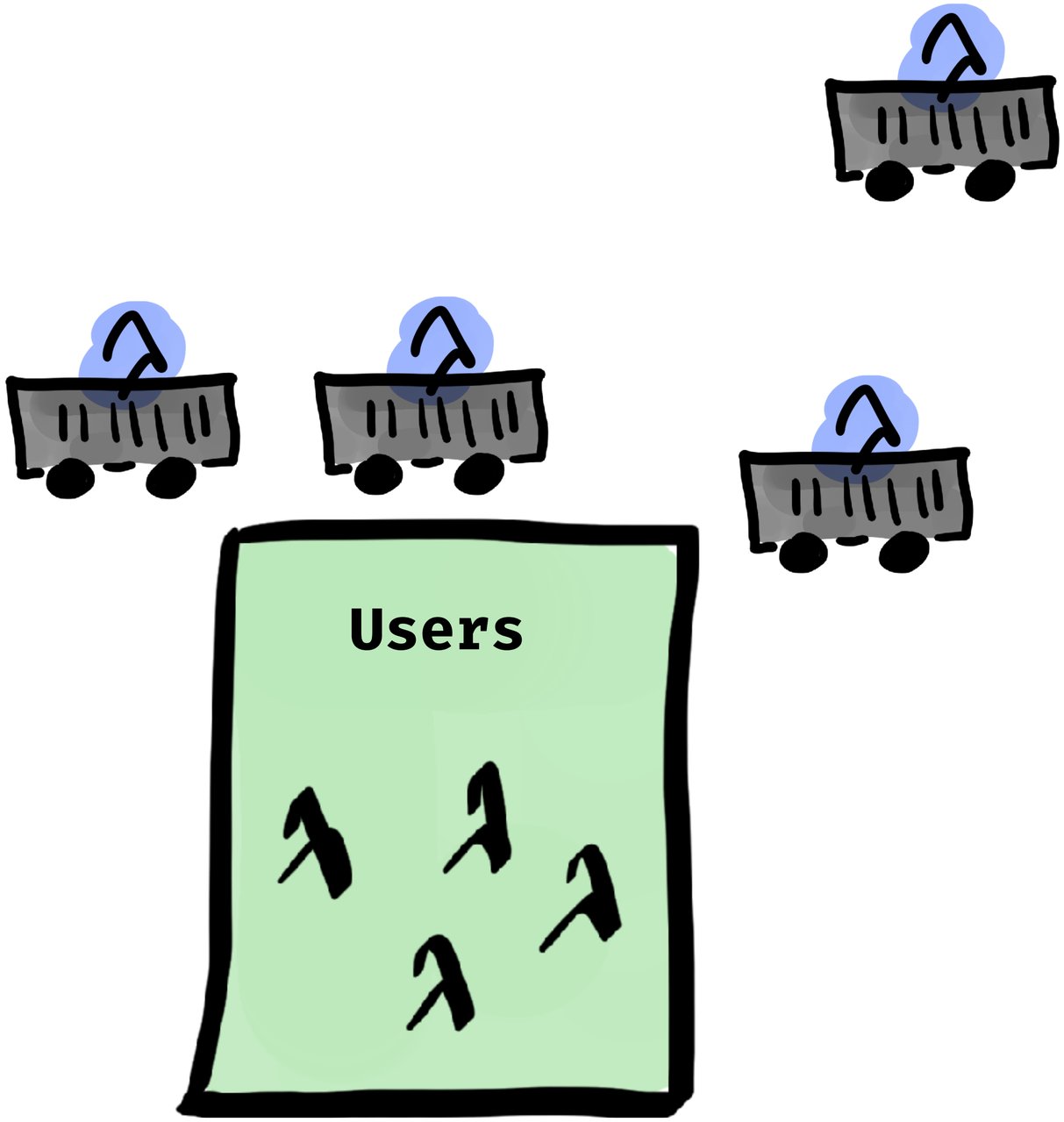
# Cold



# Cold



Cold




@Koenighotze

COLD START WILL HAPPEN

ONCE FOR EACH

CONCURRENT EXECUTION

OF YOUR FUNCTION

# WHAT CAN YOU DO?


Please help me with aws lambda cold start

Google Search I'm Feeling Lucky

# NO SLA

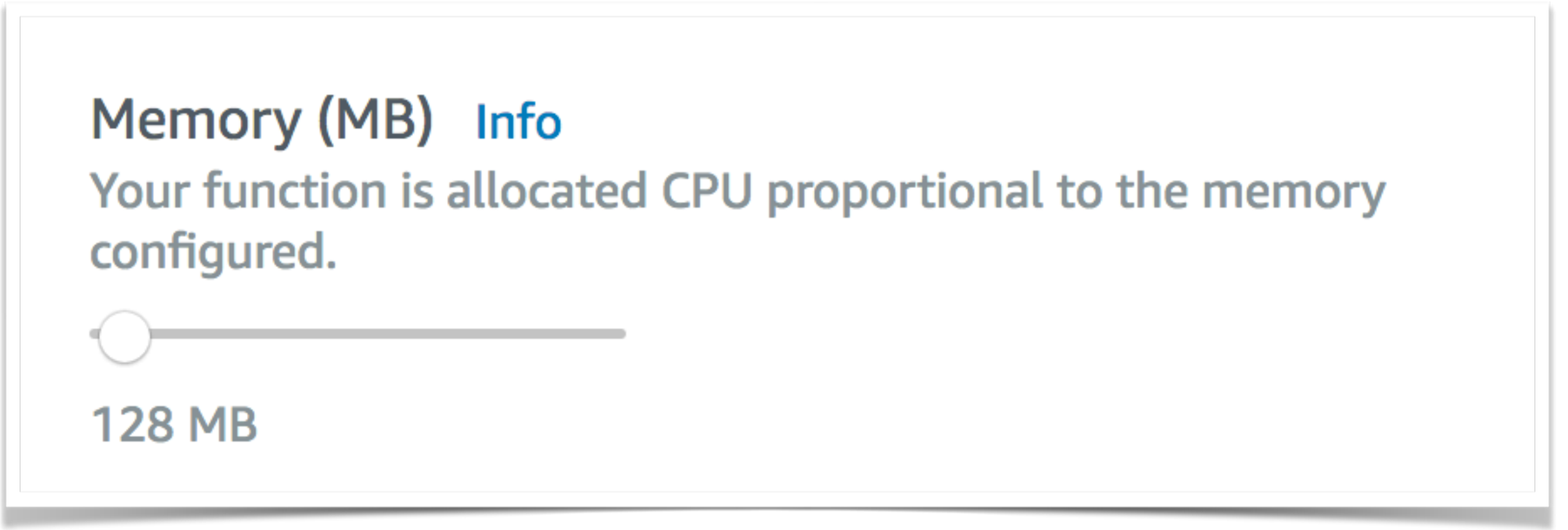
# NO HARD DETAILS
# JUST GUIDELINES

# PACKAGE SIZE?

| Function name | Description | Runtime | Code size |
| --- | --- | --- | --- |
| Fis2_0-Contract-DismissContract | Terminates a contract | Node.js 6.10 | 51.7 MB |
| Fis2_0-Contract-GetContractByEmployee | Get contract for an employee | Node.js 6.10 | 51.7 MB |
| Fis2_0-Employees-GetEmployees | Get all known employees | Node.js 6.10 | 23.9 MB |
| Fis2_0-Employees-GetEmployee | Get employee by id | Node.js 6.10 | 23.9 MB |
| Fis2_0-Employees-GetContractByEmployee | Get contract for an employee | Node.js 6.10 | 23.9 MB |

# NO OBVIOUS CORRELATION!?

# MEMORY SETTINGS?


Memory (MB) Info
Your function is allocated CPU proportional to the memory configured.
128 MB

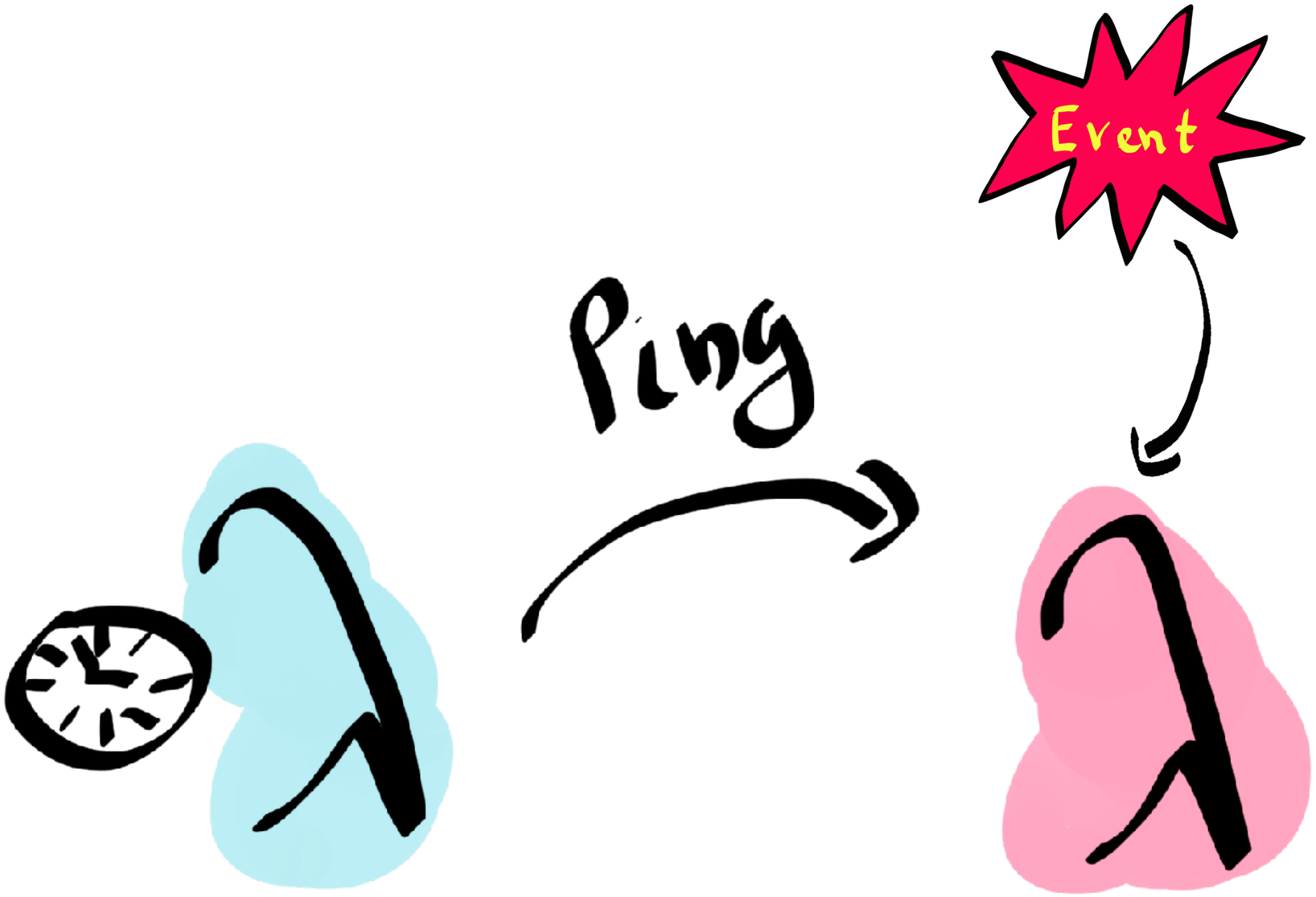
```
/AWS/LAMBDA/…REPORT
    REQUESTID:
    DURATION: 3208.99 MS
    BILLED DURATION: 3300 MS
    MEMORY SIZE: 128 MB
    MAX MEMORY USED: 59 MB
```

```
/AWS/LAMBDA/…REPORT
    REQUESTID:
    DURATION: 3208.99 MS
    BILLED DURATION: 3300 MS
    MEMORY SIZE: 128 MB
    MAX MEMORY USED: 59 MB
```

# SOME CORRELATION

# WARMUP-PING?


Ping


Event
Ping


Ping

AWS WILL KILL EVEN WARM LAMBDAS AFTER A CERTAIN TIME FRAME

# MEASURE

# CHANGE

# MEASURE

# MEASURE PERCEIVED EXTERNAL PERFORMANCE

# MEASURE USER EXPERIENCE

# DESIGN WITH LATENCY IN MIND


TIGHT SECURITY
@Koenighotze

# SERVERLESS IS GOOD FOR SECURITY

# NO LONG LIVED SERVERS OR MANUAL PATCH SCHEDULES

# …THAT YOU NEED TO HANDLE

# …BUT AMAZON DOES

# HOW DO YOU DEPLOY A WEB APPLICATION FIREWALL…

# HOW DO YOU DEPLOY A WEB APPLICATION FIREWALL…

# …WITHOUT A WEB

HOW DO YOU DEPLOY A WEB APPLICATION FIREWALL…

…WITHOUT A WEB

**…WITHOUT AN APPLICATION**

HOW DO YOU DEPLOY A WEB APPLICATION FIREWALL…

…WITHOUT A WEB

…WITHOUT AN APPLICATION

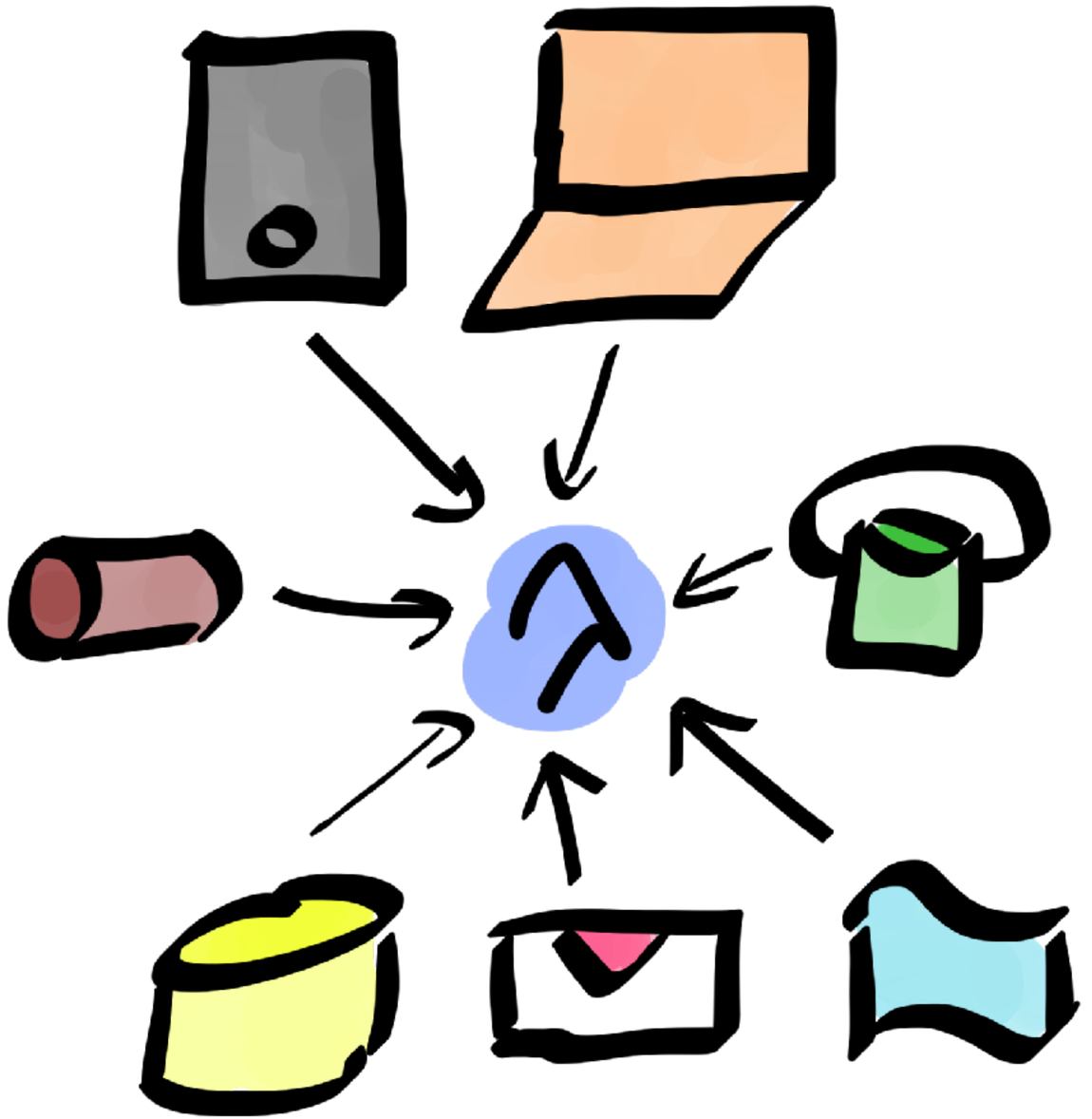
**…WITHOUT A SERVER**

# NEW OR ADAPTED

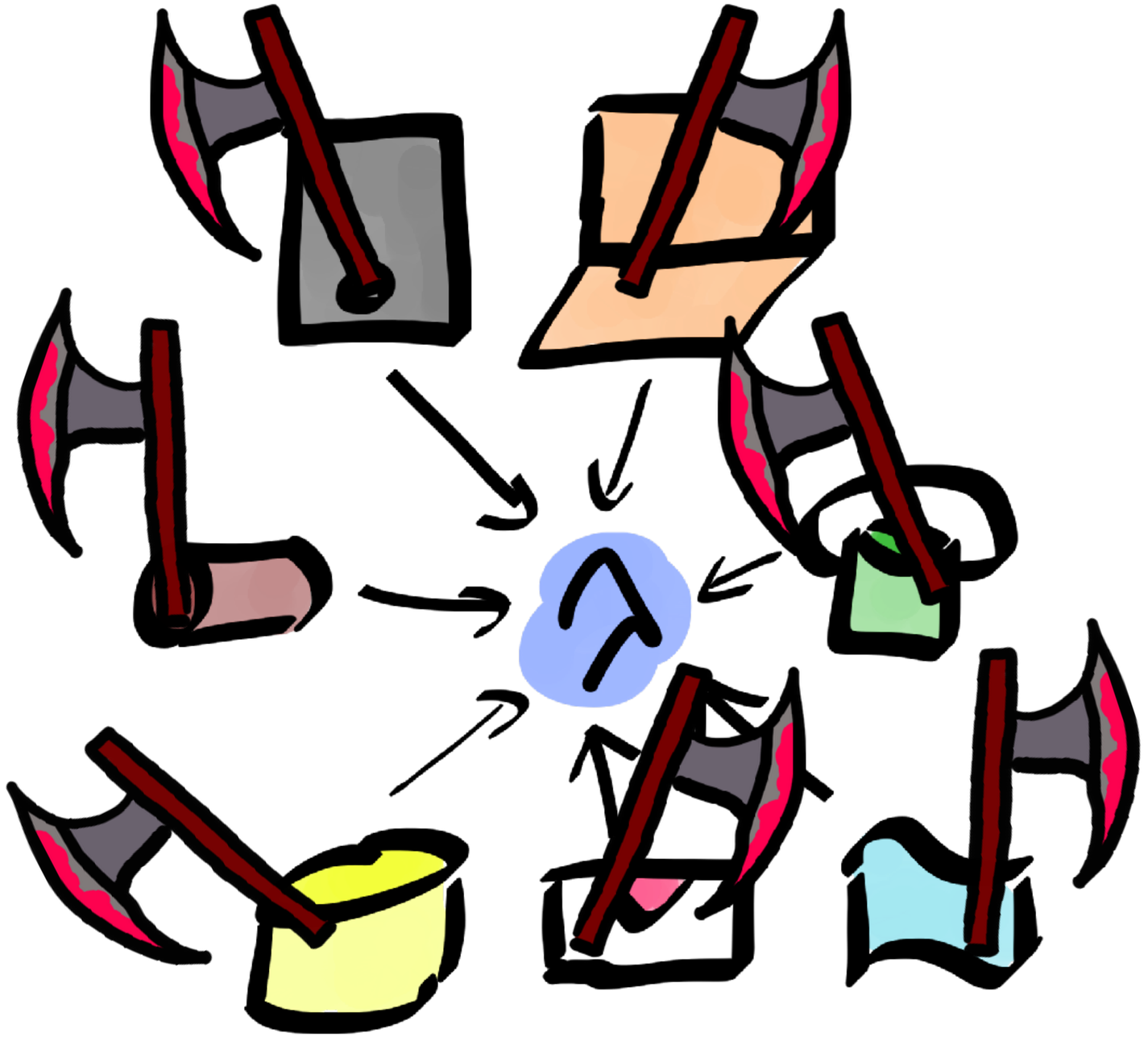
# SECURE CODING

# PATTERNS NEEDED

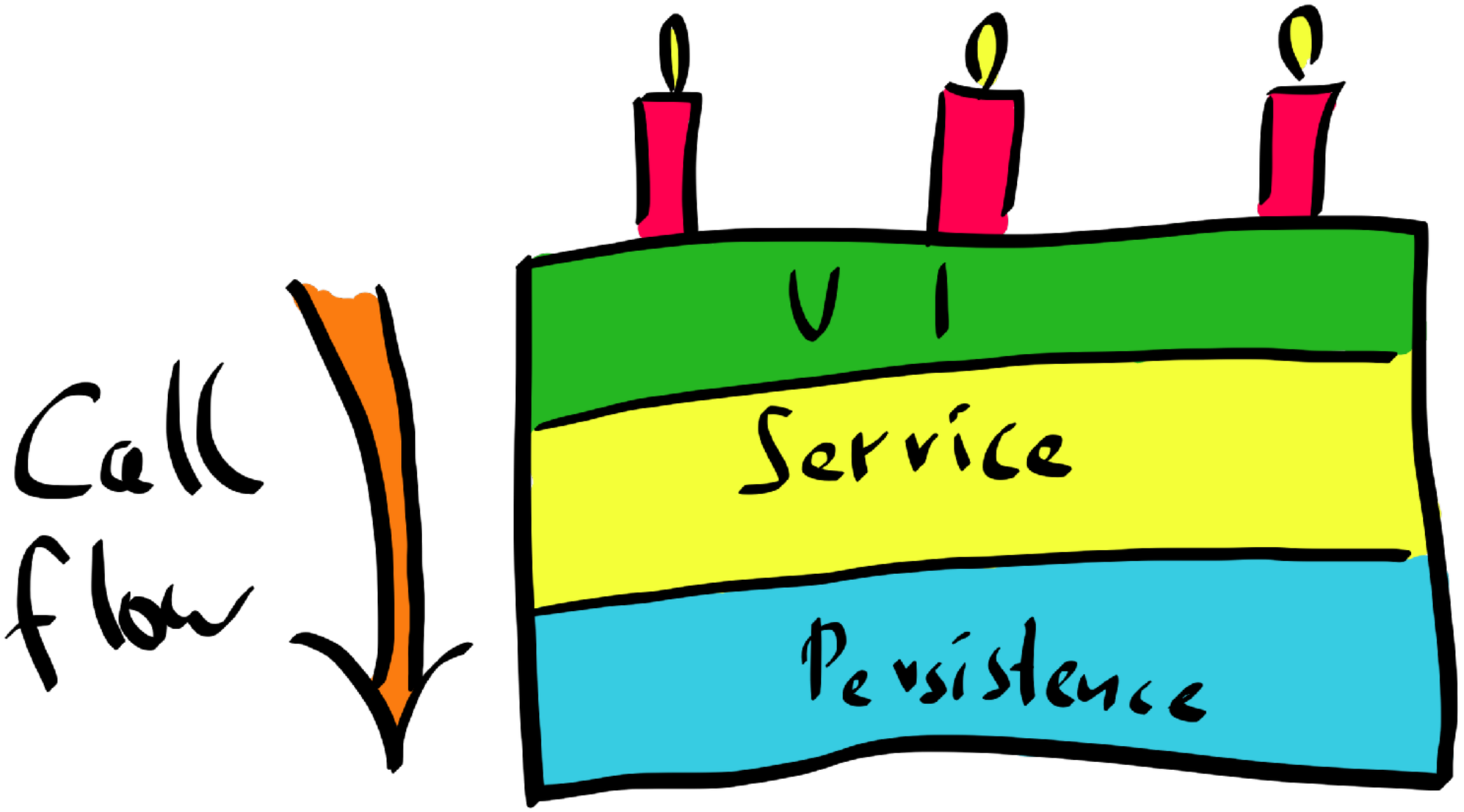
# INCREASED ATTACK SURFACE

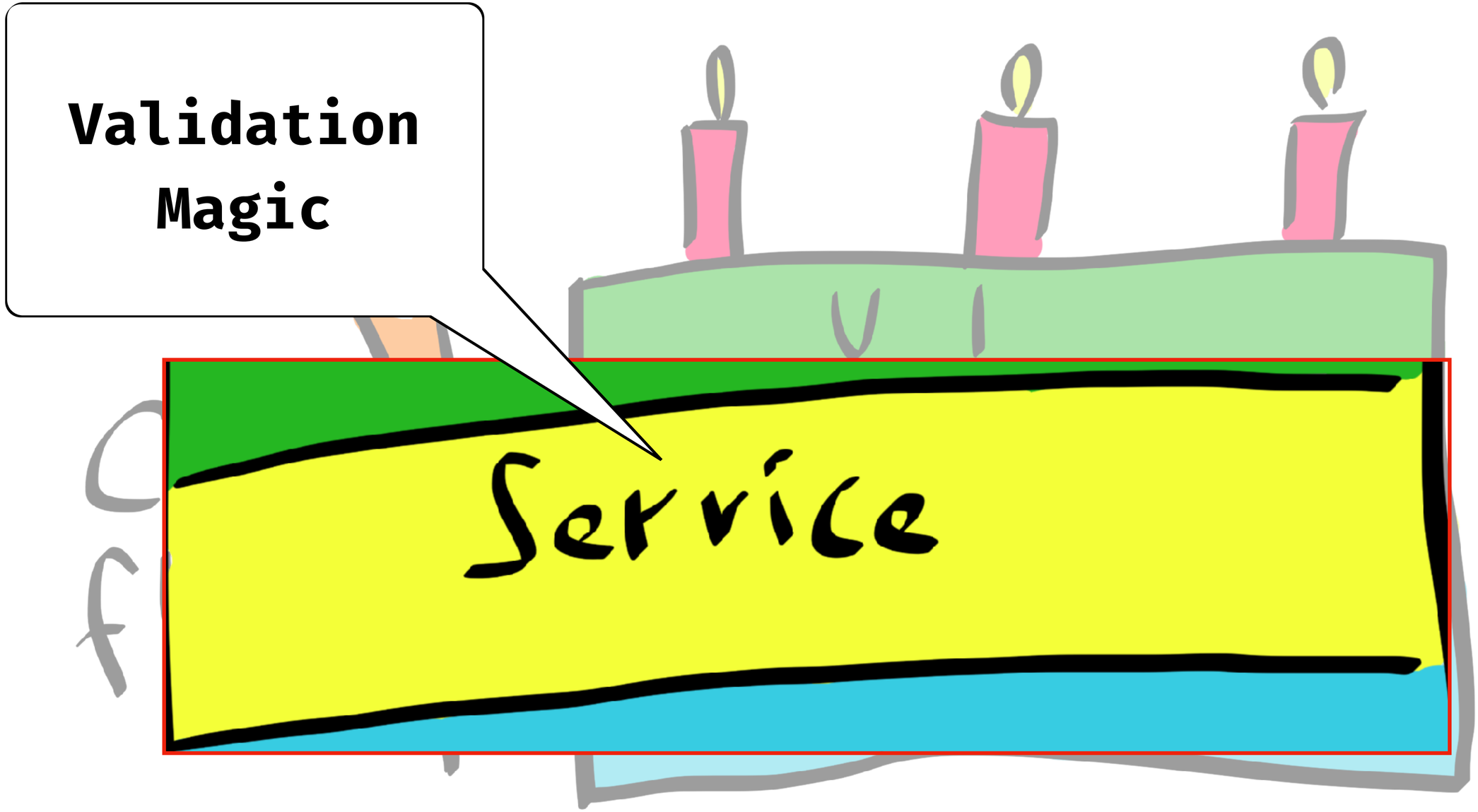


# IMAGINE EVERYBODY WANTS TO HARM YOU



# EVENT INJECTION


Call
flow
UI
Service
Persistence


Validation
Magic
Service

# CLASSIC LAYERED CAKE ARCHITECTURE DOES NOT APPLY TO SERVERLESS

# NEVER TRUST YOUR CALLER

```
const Joi = require('joi')
const eventSchema = {
  'lambdaName': Joi.string().required(),
  'invokationCount': Joi.number().required(),
  'dryRun': Joi.boolean().default(true)
}

exports.handler = (event, context, callback) => {
  const { error, value } = Joi.validate(event,  eventSchema)
  if (error) {
    return callback(new Error('Cannot parse event'))
  }

  ...doSomethingWithValue()
}
```

```
const Joi = require('joi')
const eventSchema = {
  'lambdaName': Joi.string().required(),
  'invokationCount': Joi.number().required(),
  'dryRun': Joi.boolean().default(true)
}

exports.handler = (event, context, callback) => {
  const { error, value } = Joi.validate(event,  eventSchema)
  if (error) {
    return callback(new Error('Cannot parse event'))
  }

  ...doSomethingWithValue()
}
```

```
const Joi = require('joi')
const eventSchema = {
  'lambdaName': Joi.string().required(),
  'invokationCount': Joi.number().required(),
  'dryRun': Joi.boolean().default(true)
}

exports.handler = (event, context, callback) => {
  const { error, value } = Joi.validate(event,  eventSchema)
  if (error) {
    return callback(new Error('Cannot parse event'))
  }

  ...doSomethingWithValue()
}
```

# BILLING ATTACK

# Billing Alarm

You can create a billing alarm to receive e-mail alerts when your AWS charges exceed a threshold you choose. Simply:

1. Enter a spending threshold
2. Provide an email address
3. Check your inbox for a confirmation email and click the link provided

**When my total AWS charges for the month**

**exceed:** $ 50 USD

**send a notification to:** NotifyMe New list

**Reminder:** for each address you add, you will receive an email from AWS with the subject "*AWS Notification - Subscription Confirmation*". Click the link provided in the message to confirm that AWS may deliver alerts to that address.

# SECURITY IS LIKE CSS

# NO ONE DELETES RULES

# YOU ONLY ADD RULES

# PRINCIPLE OF

# LEAST PRIVILEGES

# BEWARE CRAPPY CODE EXAMPLES

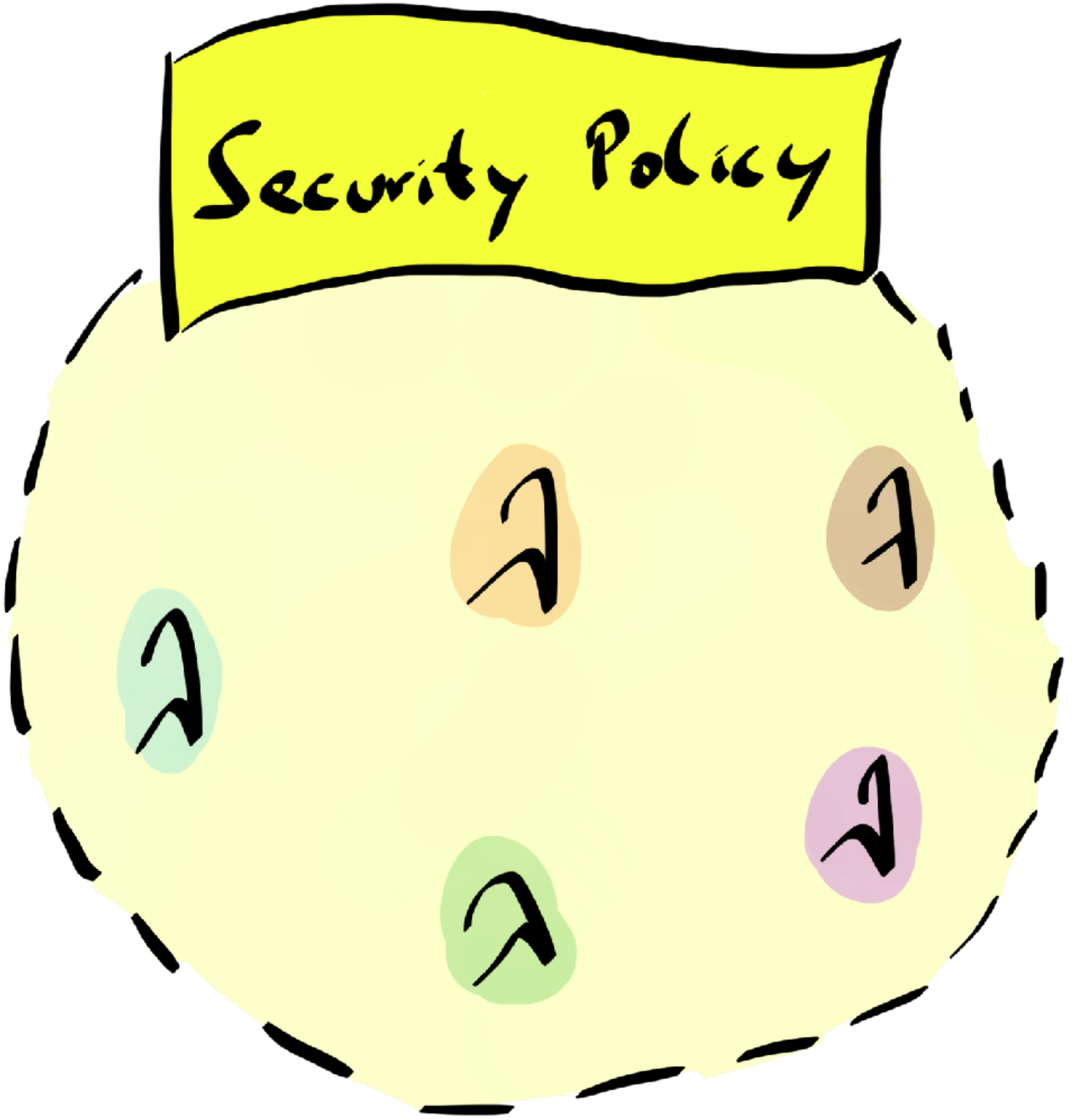
```
"Statement": [{
     "Effect": "Allow",
       "Action": [
         “s3:*",
       ],
       "Resource": [
         “arn:aws:s3:::*”
       ]
 }, …
```

```
"Statement": [{
      "Effect": "Allow",
        "Action": [
          "s3:*",
        ],
        "Resource": [
          "arn:aws:s3:::*"
        ]
 }, …
```

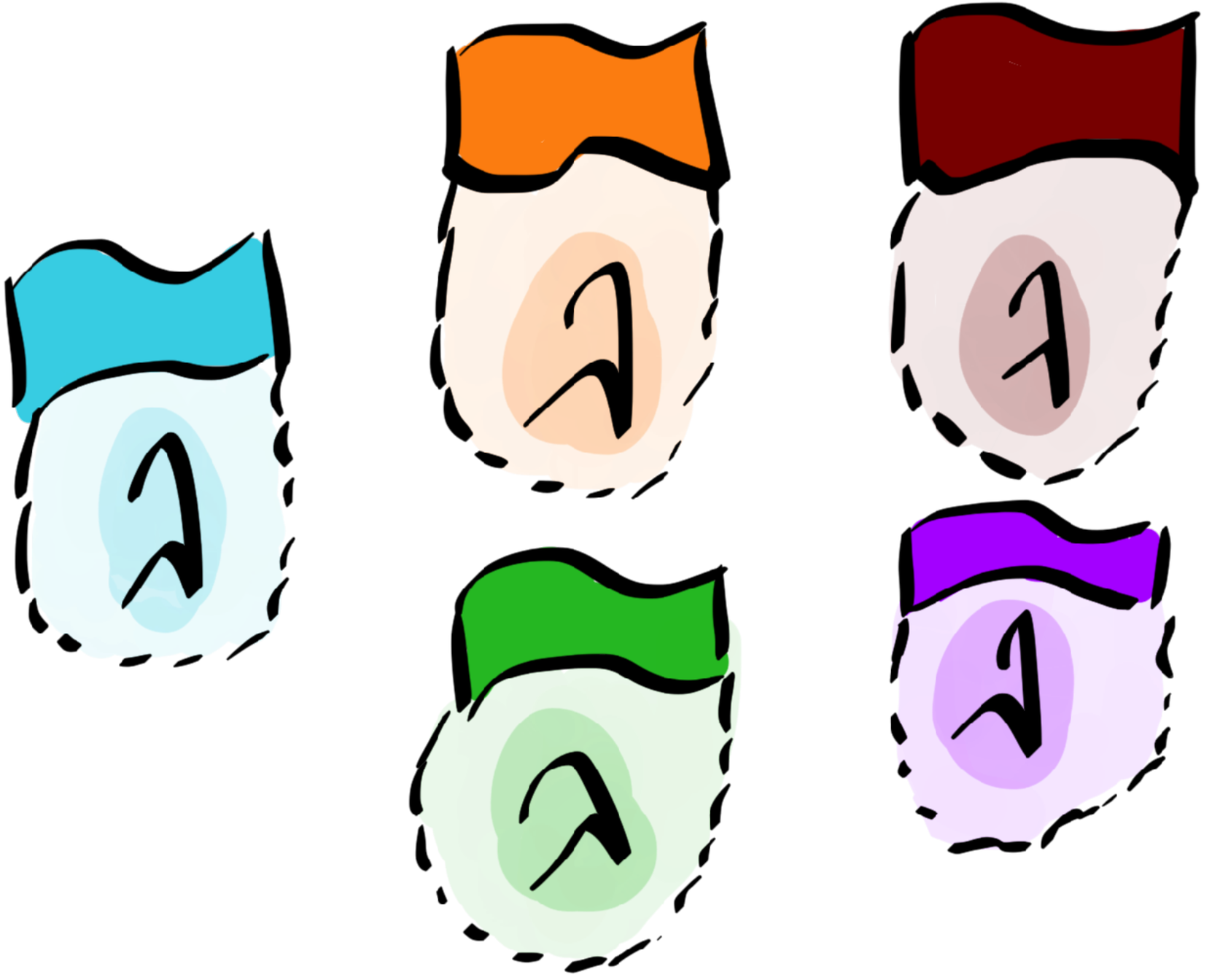
```
"Statement": [{
     "Effect": "Allow",
       "Action": [
         “s3:*",
       ],
       "Resource": [
         “arn:aws:s3:::senacor/fis/orders/*”
       ]
 }, …
```

```
"Statement": [{
     "Effect": "Allow",
       "Action": [
         "s3:GetObject"
       ],
       "Resource": [
         “arn:aws:s3:::senacor/fis/orders/*”
       ]
 }, …
```

```
"Statement": [{
      "Effect": "Allow",
        "Action": [
          "s3:GetObject"
        ],
        "Resource": [
          “arn:aws:s3:::senacor/fis/orders/*”
        ]
 }, …
```


Security Policy

# DO NOT SHARE POLICIES



# NO EXCUSES WITH PROPER TOOLING

```yaml
Resources:
  ForwardBillingRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Sub "ForwardBillingRole-${Stage}"
      AssumeRolePolicyDocument: ...
      ManagedPolicyArns: ...
      Policies:
        -
          PolicyName: !Sub "StoreBillingInS3Policy-${Stage}"
          PolicyDocument: ...

  ForwardBilling:
    Type: AWS::Serverless::Function
    Properties:
      Role: !GetAtt ForwardBillingRole.Arn
```

```yaml
Resources:
  ForwardBillingRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Sub "ForwardBillingRole-${Stage}"
      AssumeRolePolicyDocument: ...
      ManagedPolicyArns: ...
      Policies:
        -
          PolicyName: !Sub "StoreBillingInS3Policy-${Stage}"
          PolicyDocument: ...

  ForwardBilling:
    Type: AWS::Serverless::Function
    Properties:
      Role: !GetAtt ForwardBillingRole.Arn
```

```yaml
Resources:
  ForwardBillingRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Sub "ForwardBillingRole-${Stage}"
      AssumeRolePolicyDocument: ...
      ManagedPolicyArns: ...
      Policies:
        -
          PolicyName: !Sub "StoreBillingInS3Policy-${Stage}"
          PolicyDocument: ...

  ForwardBilling:
    Type: AWS::Serverless::Function
    Properties:
      Role: !GetAtt ForwardBillingRole.Arn
```

```yaml
Resources:
  ForwardBillingRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Sub "ForwardBillingRole-${Stage}"
      AssumeRolePolicyDocument: ...
      ManagedPolicyArns: ...
      Policies:
        -
          PolicyName: !Sub "StoreBillingInS3Policy-${Stage}"
          PolicyDocument: ...

  ForwardBilling:
    Type: AWS::Serverless::Function
    Properties:
      Role: !GetAtt ForwardBillingRole.Arn
```

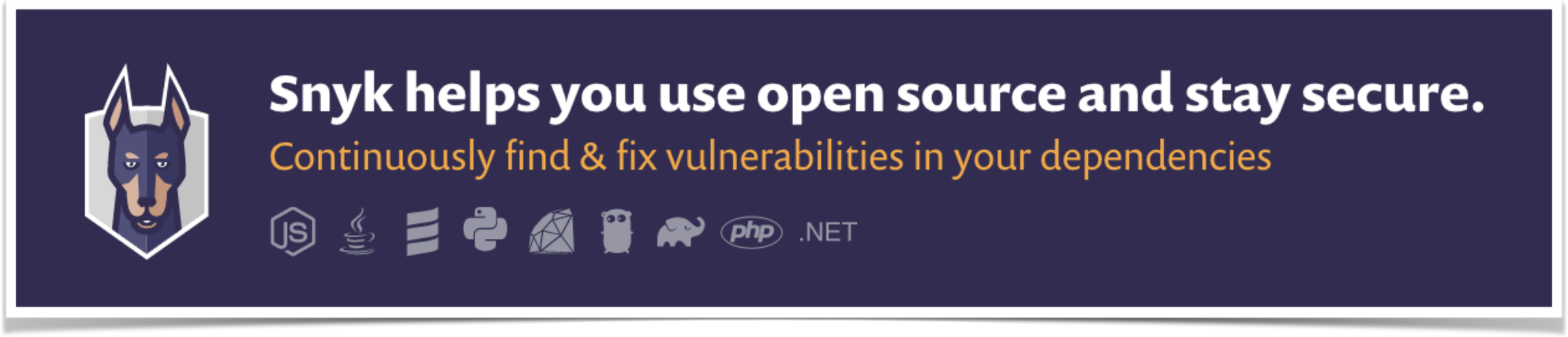
# USE A SECURITY

# WATCHDOG

# YOUR FUNCTION MAY BE SMALL, BUT YOUR DEPENDENCIES MAY NOT

```
$ du -s src/
8.0K src/

$ ls -lh lambda.zip
7.6M Mar  1 07:13 lambda.zip
```

```
$ du -s src/
8.0K src/

$ ls -lh lambda.zip
7.6M Mar  1 07:13 lambda.zip
```


Snyk helps you use open source and stay secure.
Continuously find & fix vulnerabilities in your dependencies
JS
php
.NET

# Where is the code you want to test?

Choose from the sources connected to your organisation:

GitHub

AWS Lambda

Source not shown? Browse available integrations

18:42 **snyk-bot** APP

**New remediation for Prototype Pollution**

New upgrade to address this vulnerability in package `hoek`.

Affects project senacor-aktuelles in organisation koenighotze.

Fix with CLI snyk wizard.

| Remediation | Package |
| --- | --- |
| Upgrade | hoek |
| **Project** | **Version** |
| senacor-aktuelles | 4.2.0 |

# serverless-puresec-cli


Website • Newsletter • Twitter

Serverless plugin for PureSec CLI.

## Features

- Saves you time - magically creates IAM roles for you
- Reduces the attack surface of your AWS Lambda based application
- Helps create least privileged roles with the minimum required permissions
- Currently supported runtimes: Node.js, Python (more runtimes coming soon...)
- Currently supported services: DynamoDB, Kinesis, KMS, Lambda, S3, SES, SNS & Step Functions
- Works with the Serverless Framework

# SECURITY MUST BE PART OF DEVELOPMENT RIGHT FROM THE START

# YOU BUILD IT

# YOU RUN IT

# YOU BUILD IT
# YOU SECURE IT
# AND THEN RUN IT


NEW ARCHITECTURES
NEW TRAPS
@Koenighotze

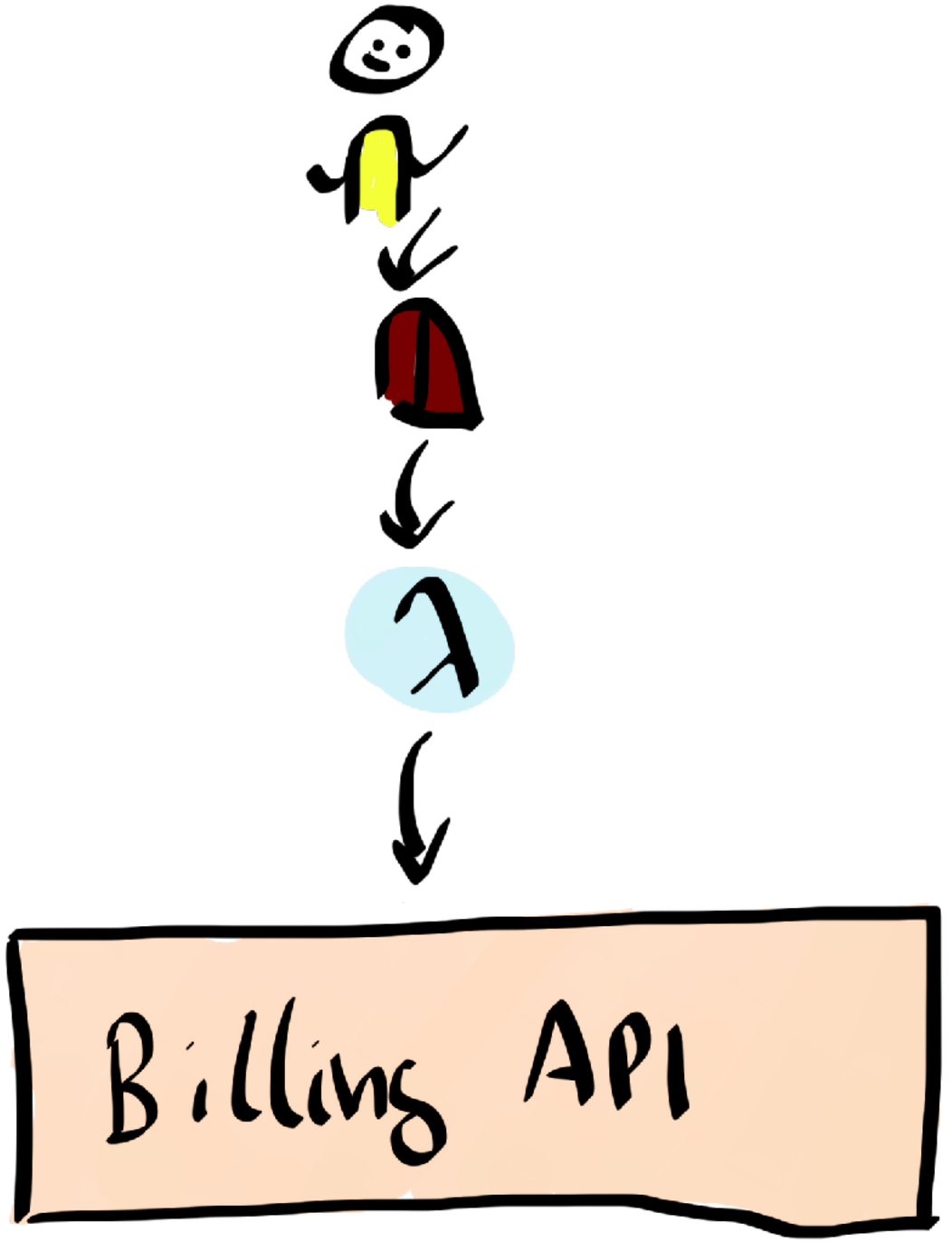

@Koenighotze

# BEWARE OF KILLING YOUR VINTAGE BACKENDS

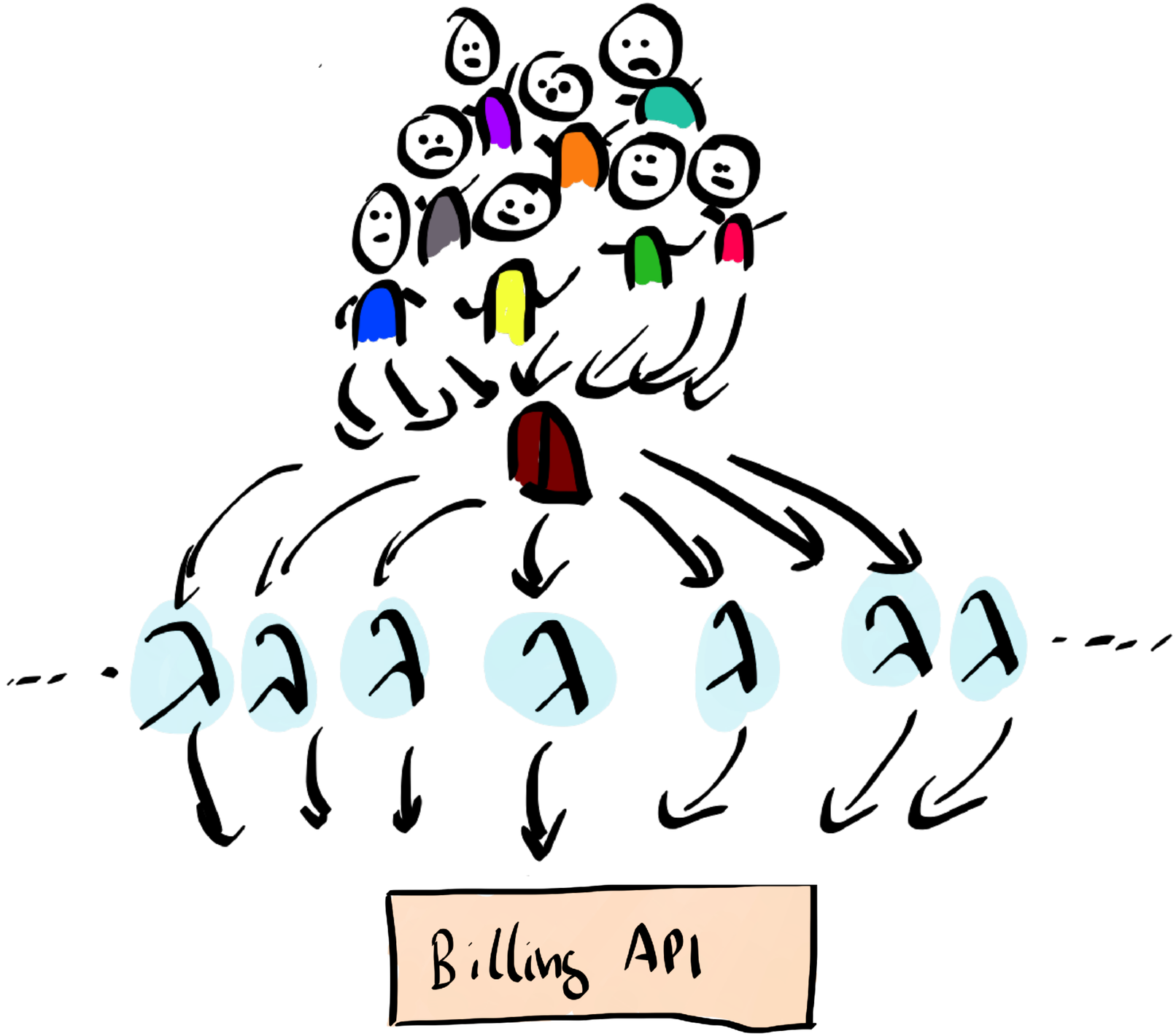
# LAMBDA SCALES BY REQUEST

# …YOUR BACKEND PROBABLY DOES NOT

# “Billings are submitted using our legacy API”


λ
Billing API

# …AND AT THE END OF A MONTH…


Billing API

Please stop this lambda non-sense

But the HYPE!

Grigoriy Myasoyedov.1897

SENACOR

@Koenighotze

# ALWAYS USE

# CONCURRENCY LIMITS

```
aws lambda put-function-concurrency
    --function-name <NAME>
    --reserved-concurrent-executions <N>
```

```
aws lambda put-function-concurrency
    --function-name <NAME>
    --reserved-concurrent-executions <N>
```

# KEEP AN EYE ON METRIC FOR CONCURRENCY FAILURES

# BE AWARE BOTTLENECKS TEND TO MOVE UPWARDS

# PREFER ASYNCHRONOUS INTEGRATION


ATTACK OF SELF DENIAL
@Koenighotze

# CONCURRENCY IS LIMITED

# BE AWARE OF

# PER ACCOUNT LIMITS

### AWS Lambda Resource Limits per Invocation

| Resource | Limits |
|---|---|
| Memory allocation range | Minimum = 128 MB / Maximum = 3008 MB (with 64 MB increments). If the maximum memory use is exceeded, function invocation will be terminated. |
| Ephemeral disk capacity ("/tmp" space) | 512 MB |
| Number of file descriptors | 1,024 |
| Number of processes and threads (combined total) | 1,024 |
| Maximum execution duration per request | 300 seconds |
| Invoke request body payload size (RequestResponse/synchronous invocation) | 6 MB |
| Invoke request body payload size (Event/asynchronous invocation) | 128 K |

### AWS Lambda Account Limits Per Region

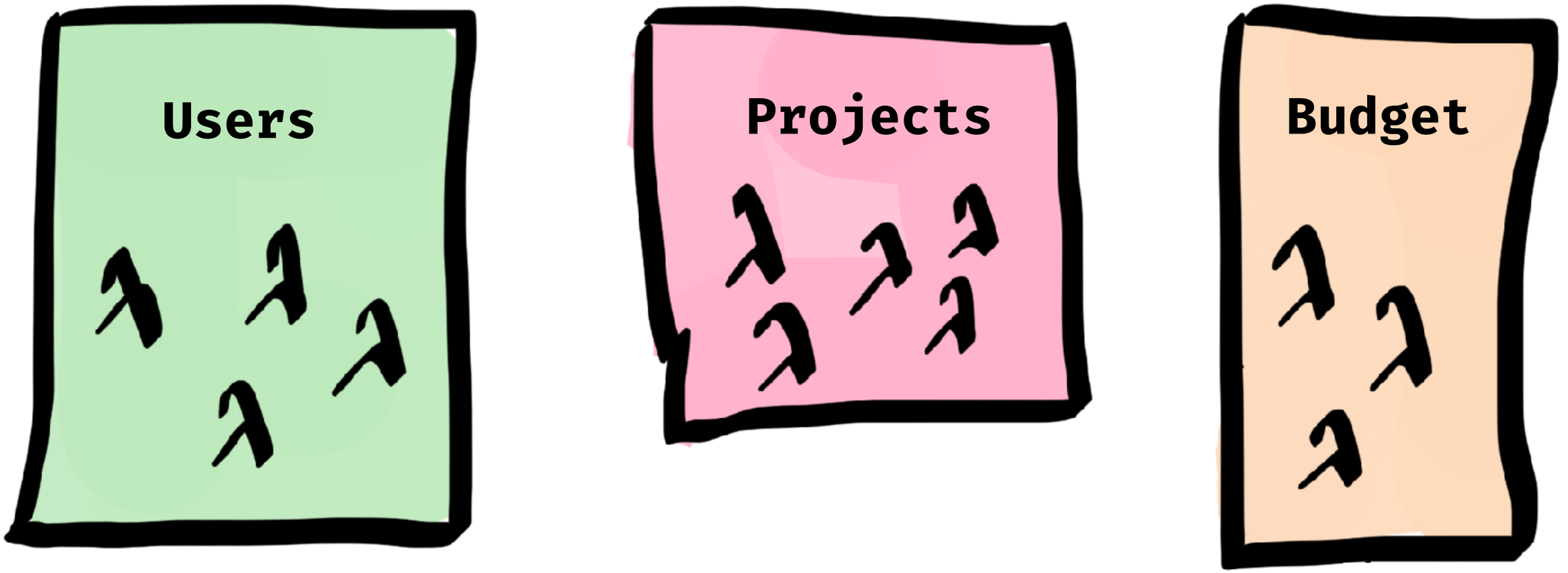
| Resource | Default Limit |
|---|---|
| Concurrent executions (see Managing Concurrency) | 1000 |

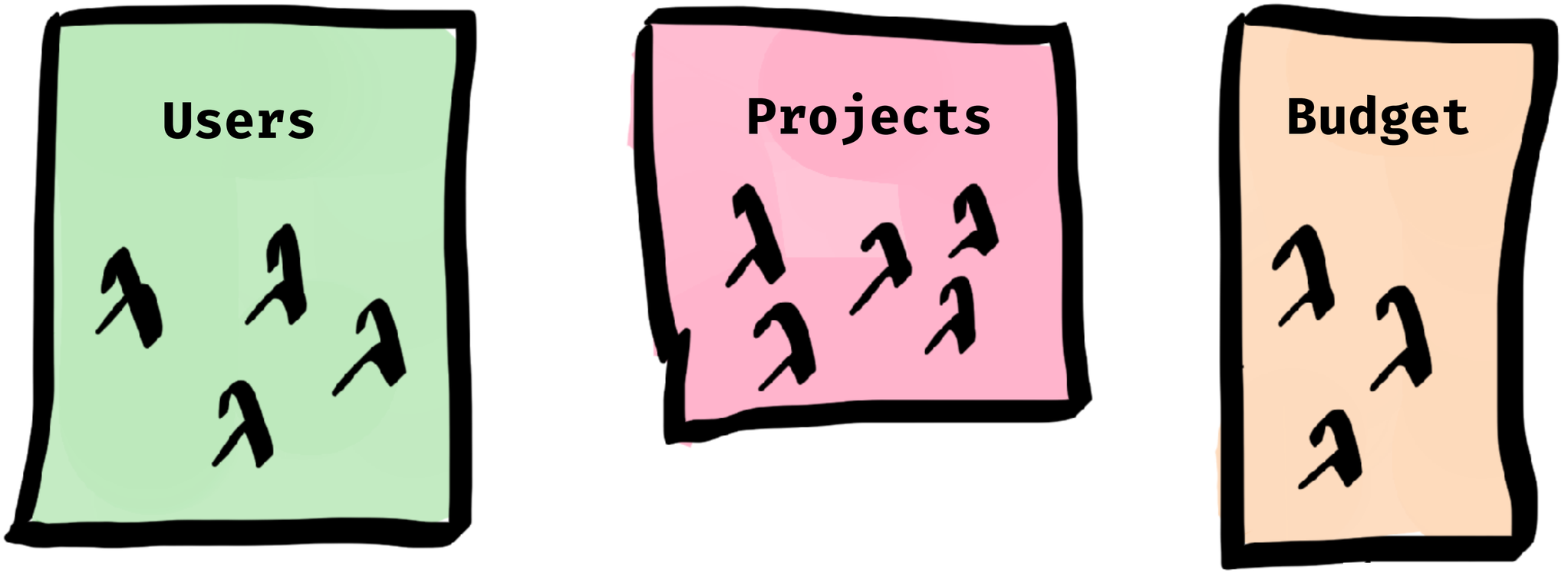
### AWS Lambda Resource Limits per Invocation

| Resource | Limits |
|---|---|
| Memory allocation range | Minimum = 128 MB / Maximum = 3008 MB (with 64 MB increments). If the maximum memory use is exceeded, function invocation will be terminated. |
| Ephemeral disk capacity ("/tmp" space) | 512 MB |
| Number of file descriptors | 1,024 |
| Number of processes and threads (combined total) | 1,024 |
| Maximum execution duration per request | 300 seconds |
| Invoke request body payload size (RequestResponse/synchronous invocation) | 6 MB |
| Invoke request body payload size (Event/asynchronous invocation) | 128 K |

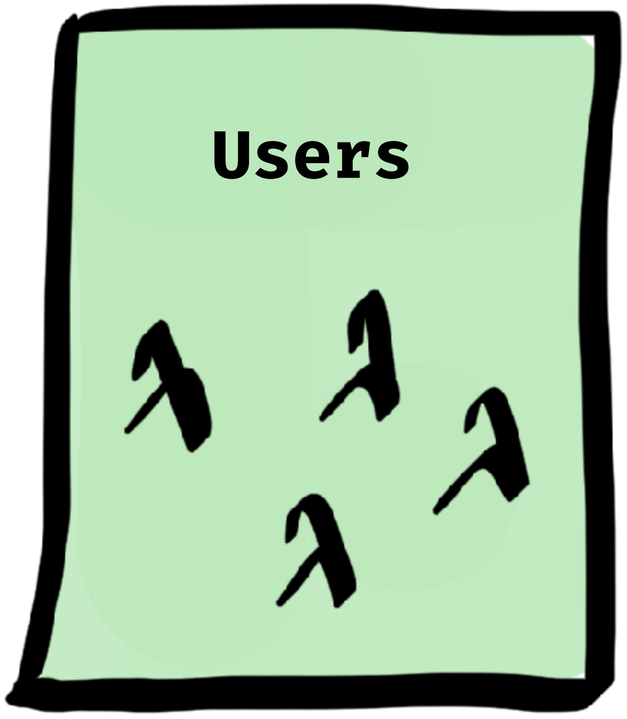
AW

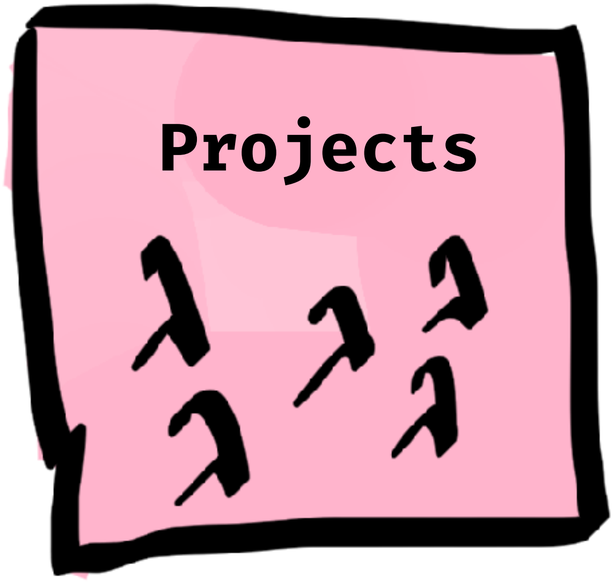
| Resource | Default Limit |
|---|---|
| Concurrent executions (see Managing Concurrency) | 1000 |

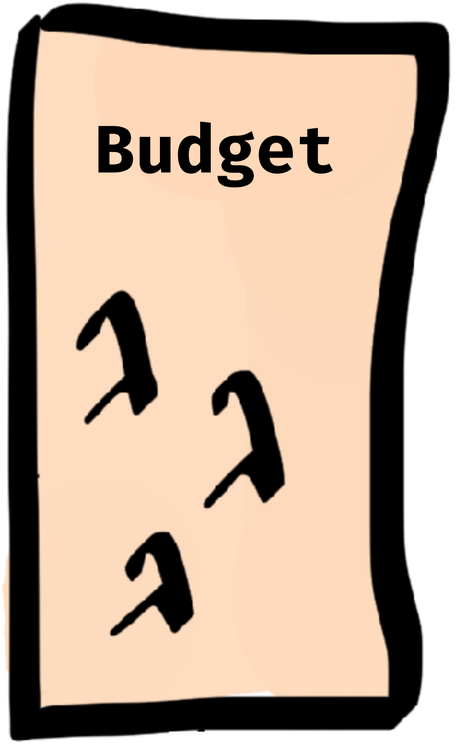

Users
Projects
Budget

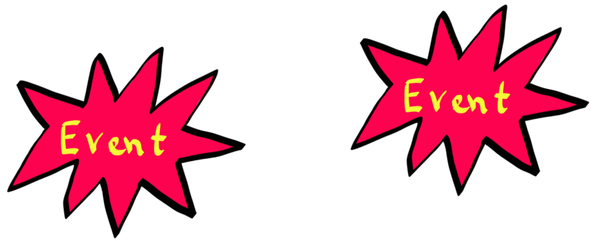

Users
Projects
Budget


Event

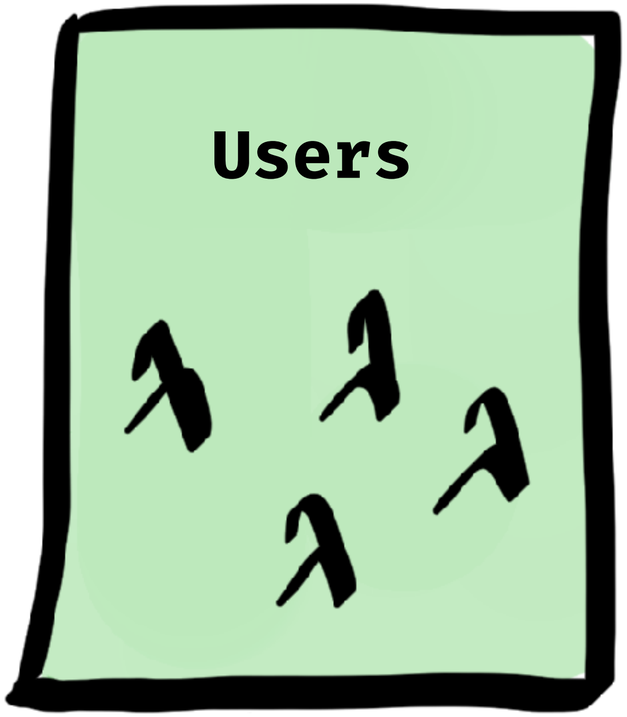

Users

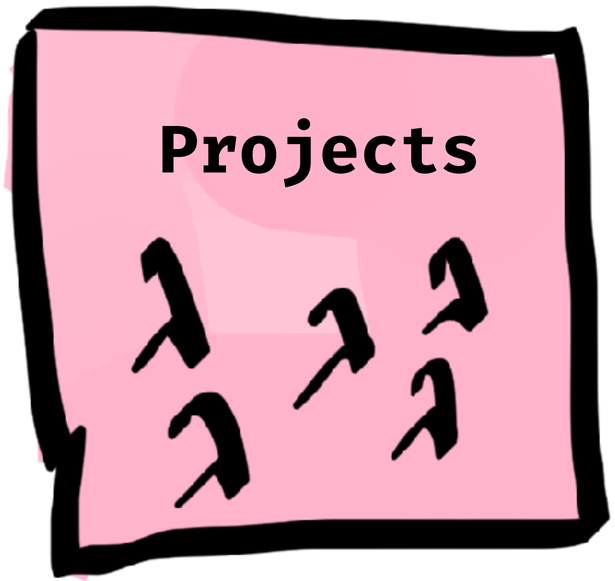

Projects

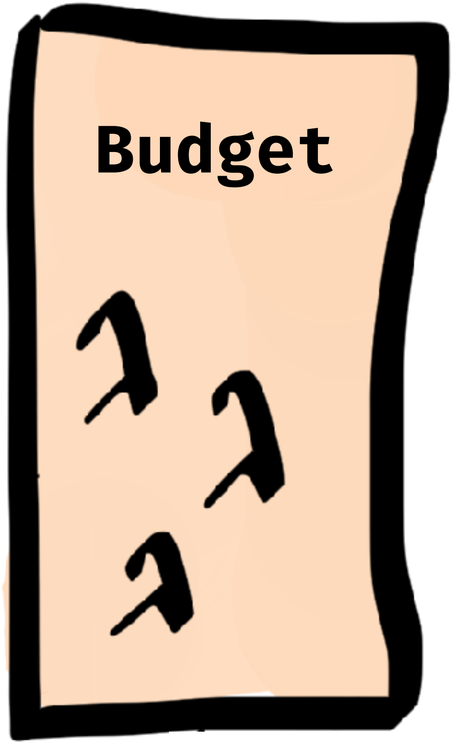

Budget

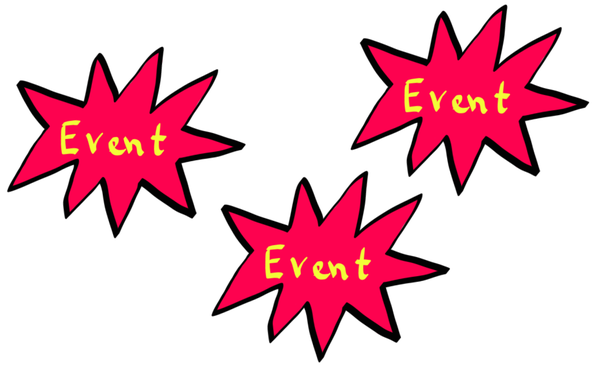

Event

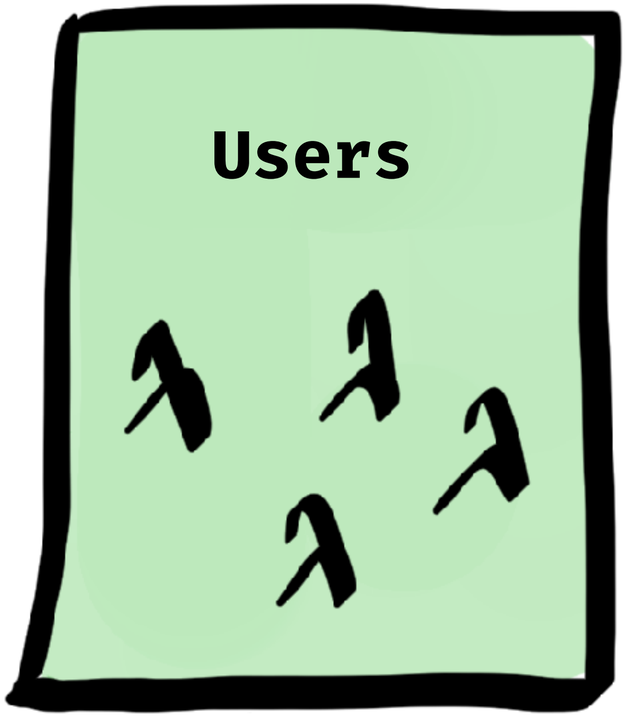

Event

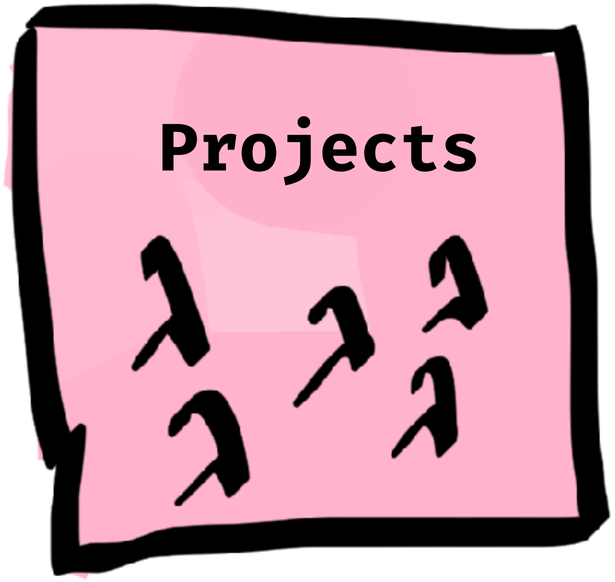

Users

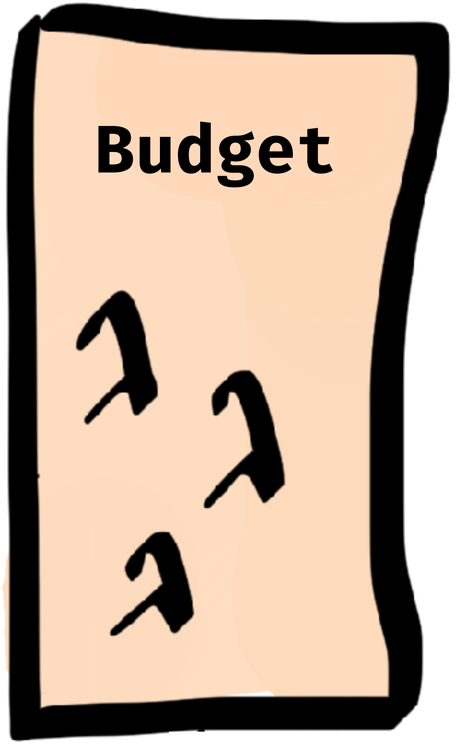

Projects


Budget

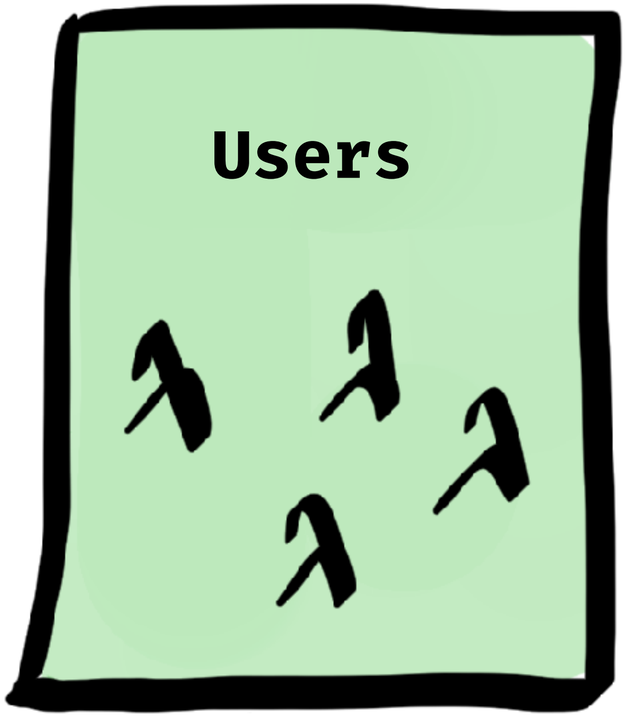

Event
Event
Event

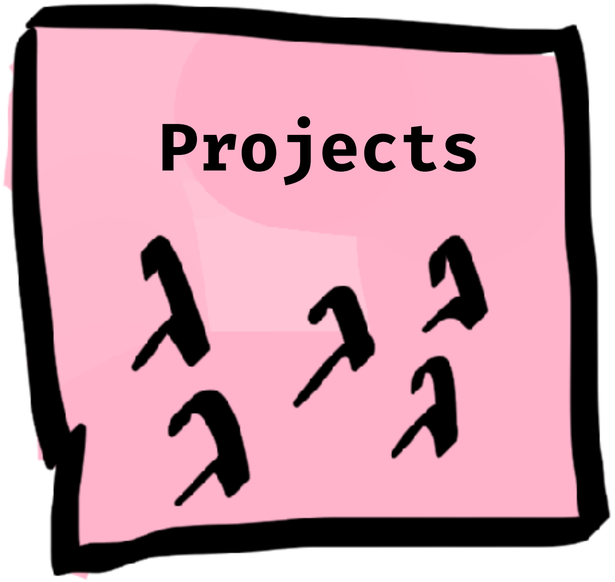

Users

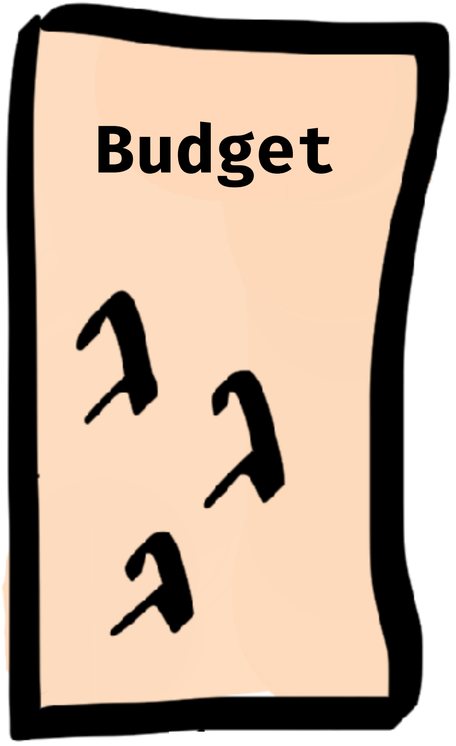

Projects


Budget

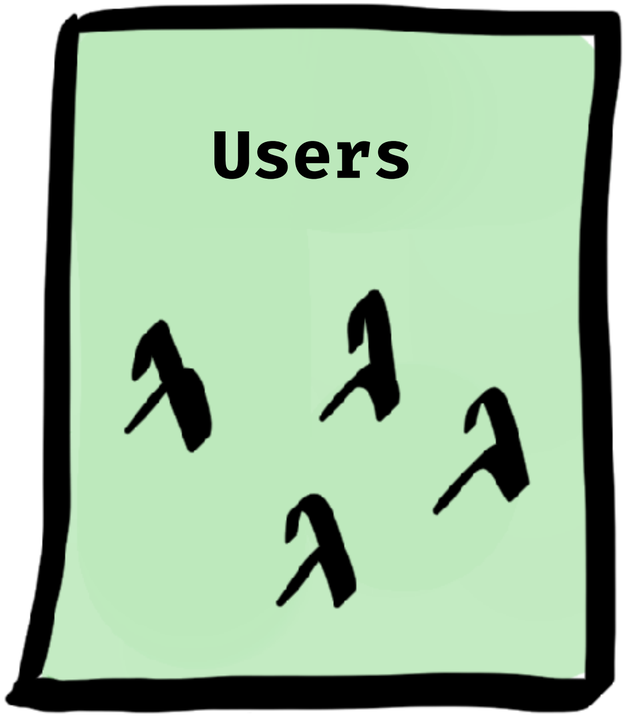

Event
Event
Event
Event

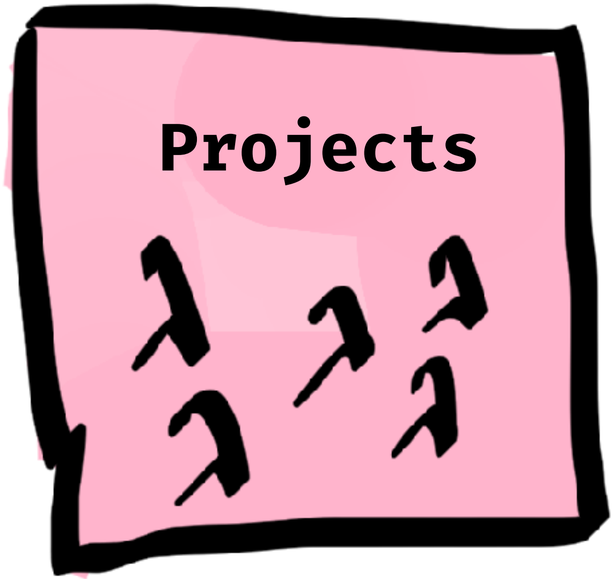

Users

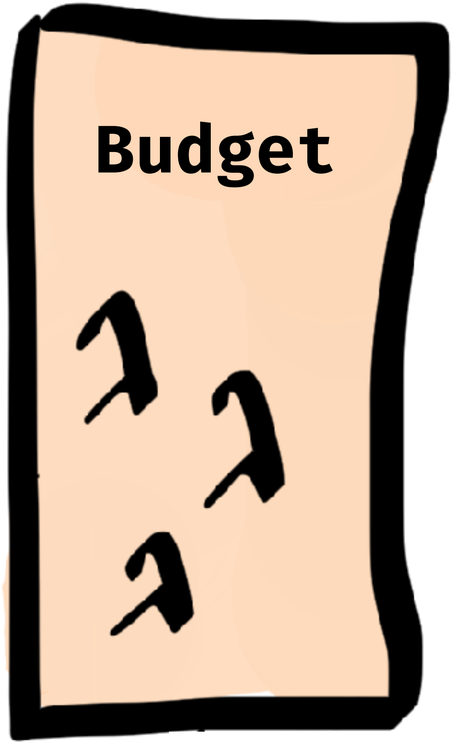

Projects


Budget

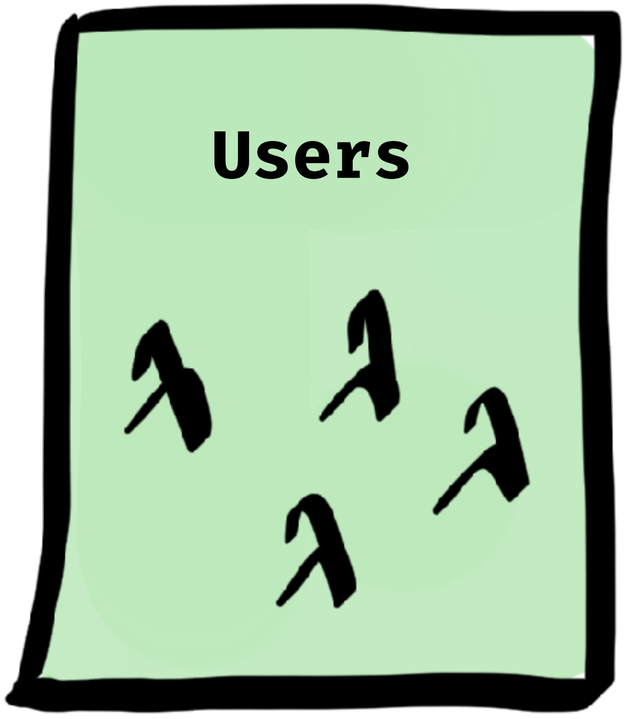

Event
Event
Event
Event

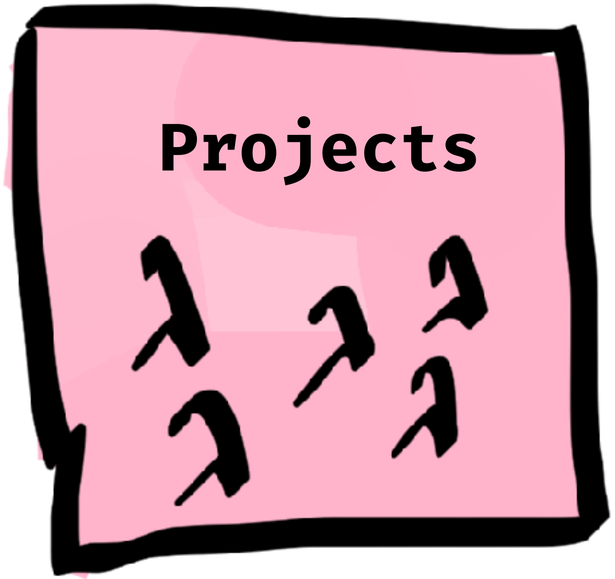

Users

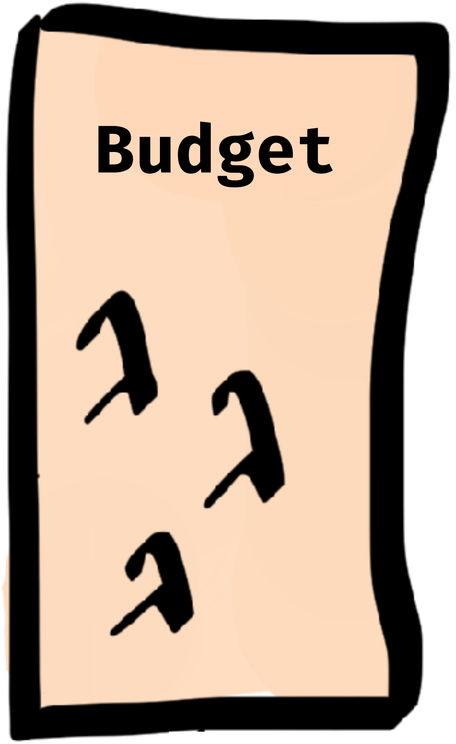

Projects

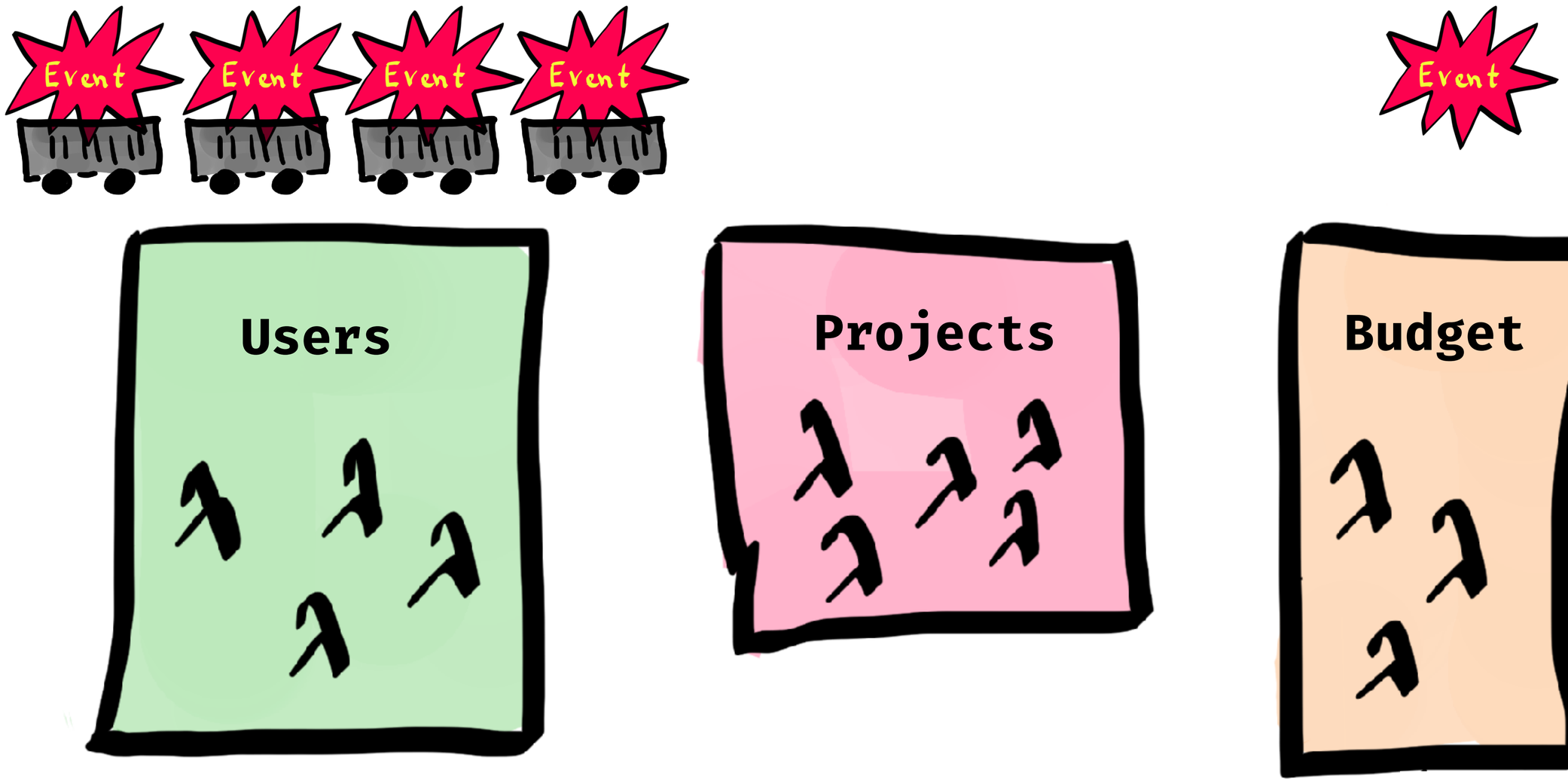

Budget

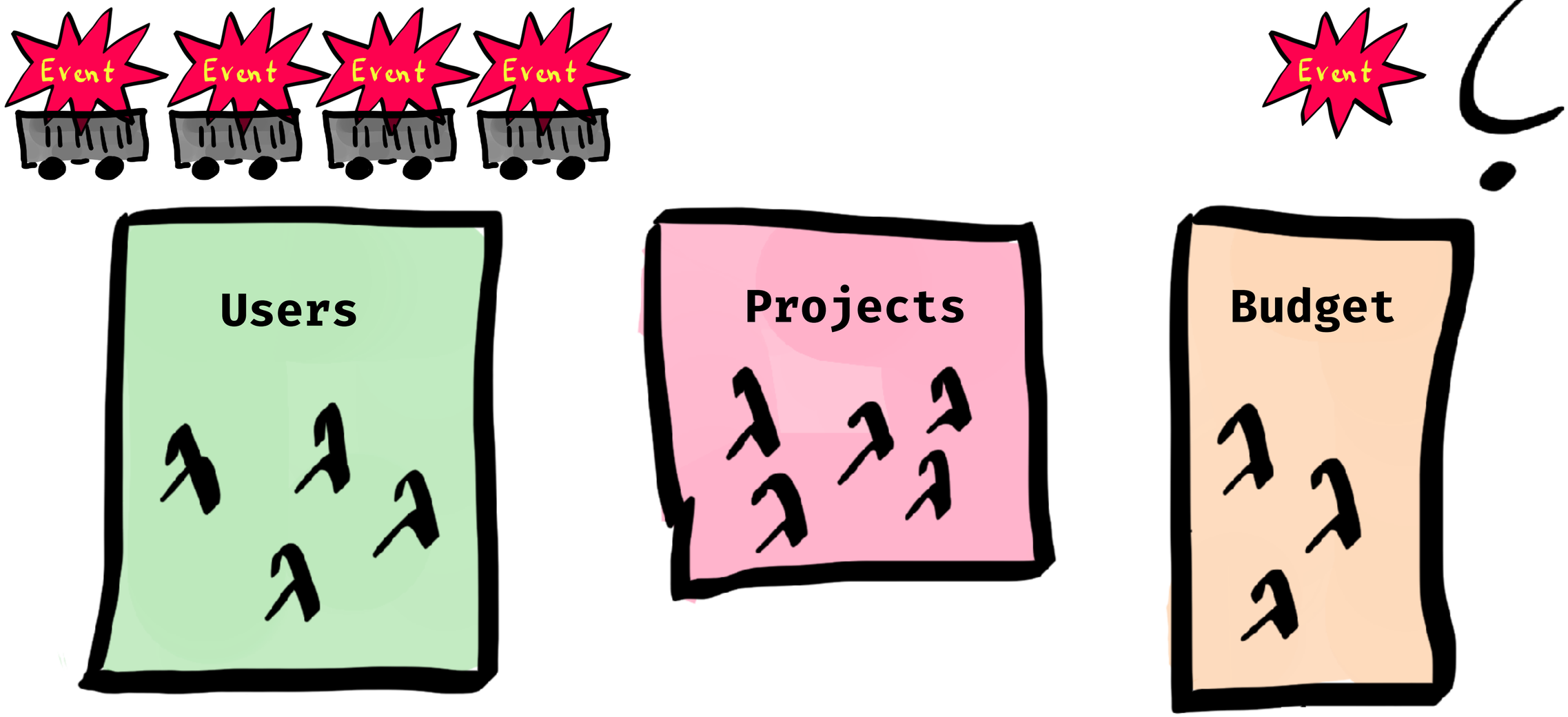

Event
Event
Event
Event


Users


Projects

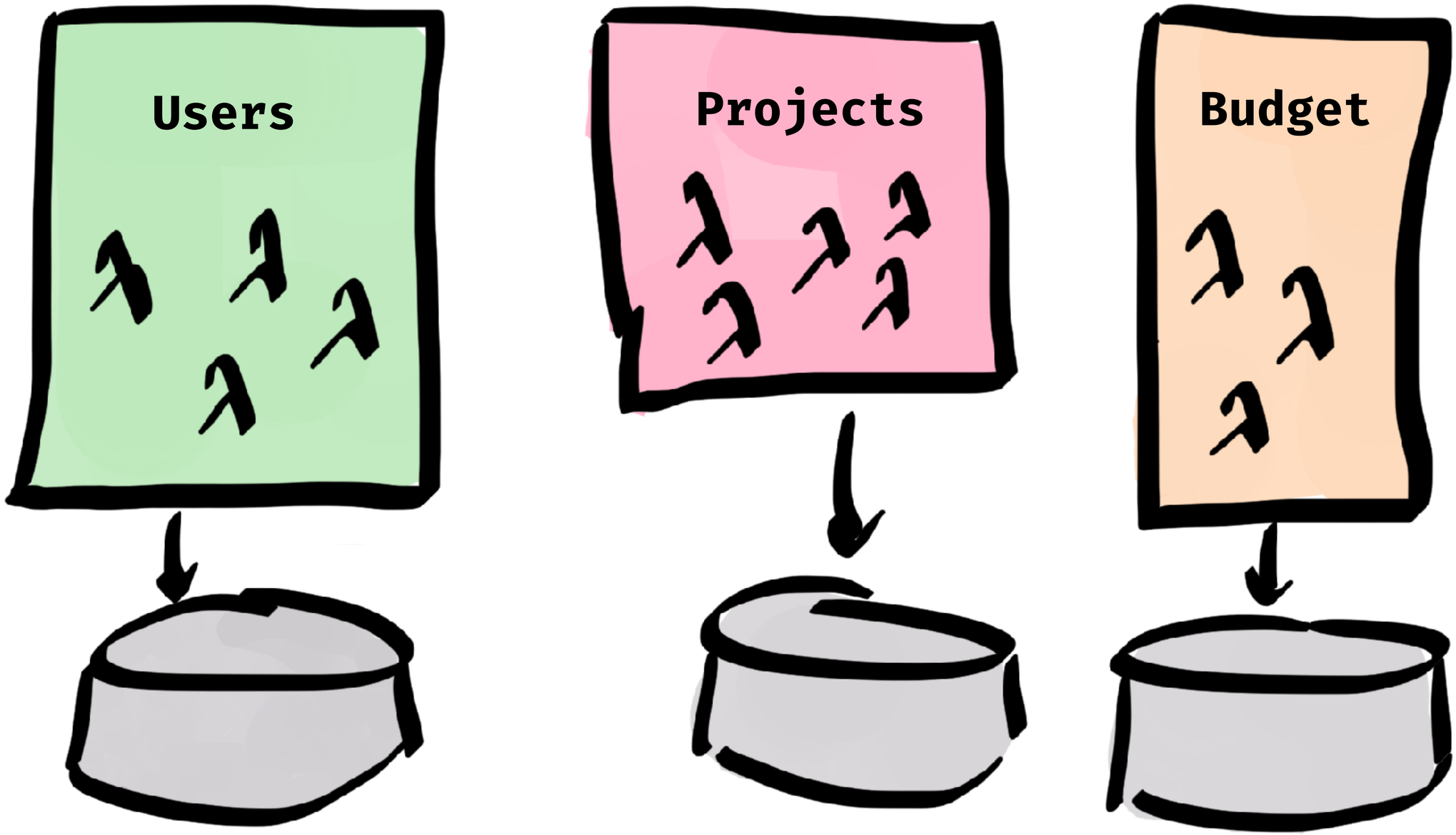

Budget


Event
Event
Event
Event
Event
Users
Projects
Budget

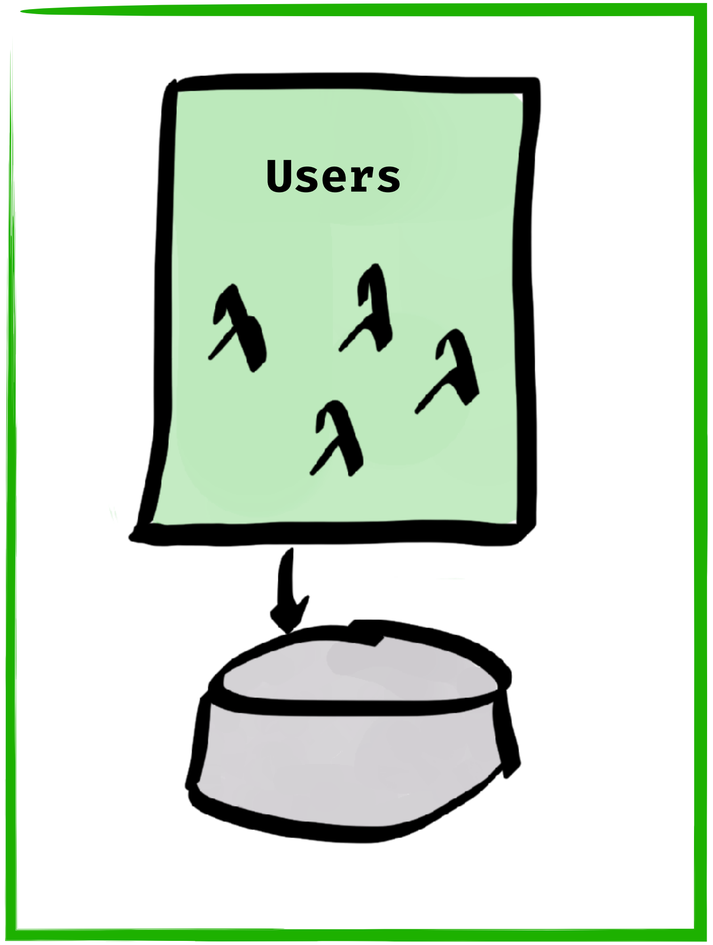

Event
Event
Event
Event
Event
Users
Projects
Budget

# USE MULTIPLE ACCOUNTS

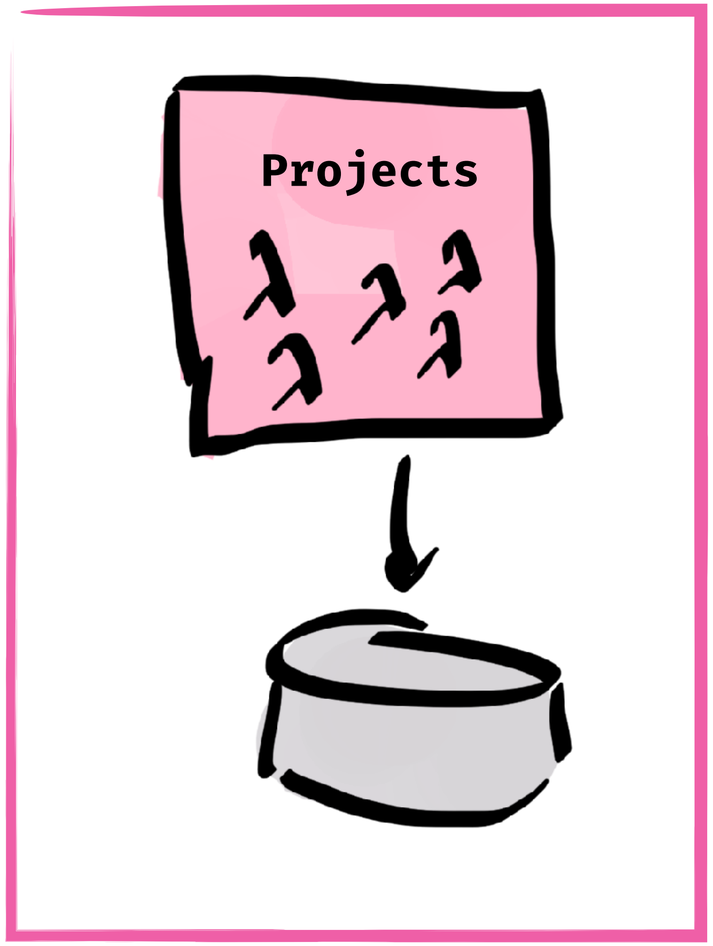
# SPLIT PER BOUNDED CONTEXT


Users
Projects
Budget

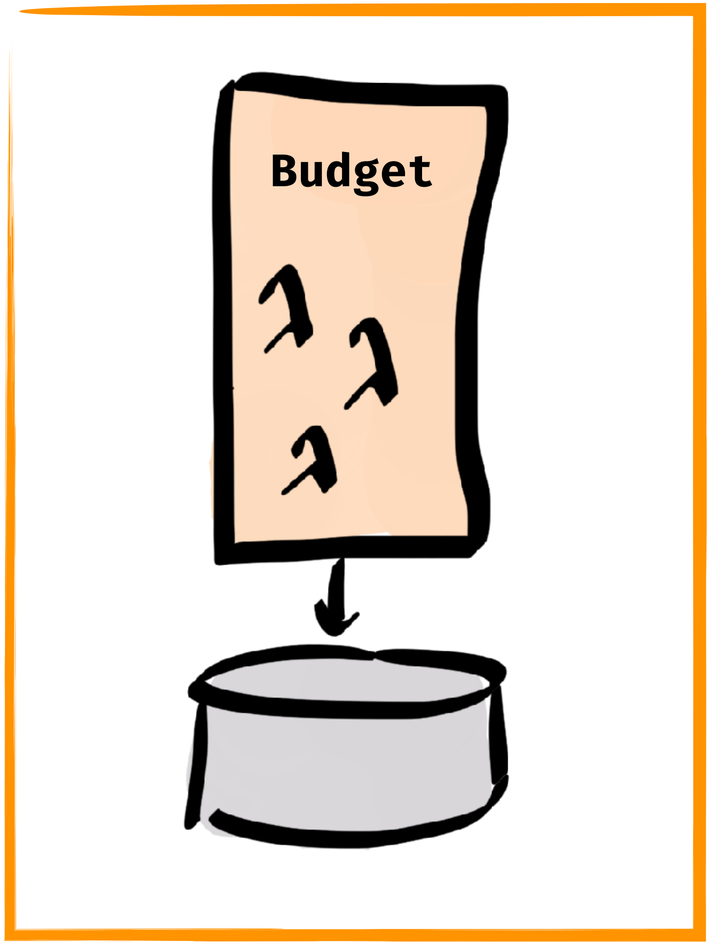
## Users Account




## Project Account




## Budget Account




PATTERNS, SHARING,
DEPENDENCIES
@Koenighotze

# ONE LAMBDA WITH DISPATCH

ONE LAMBDA WITH DISPATCH

**MULTI LAMBDA - SHARED ZIP**

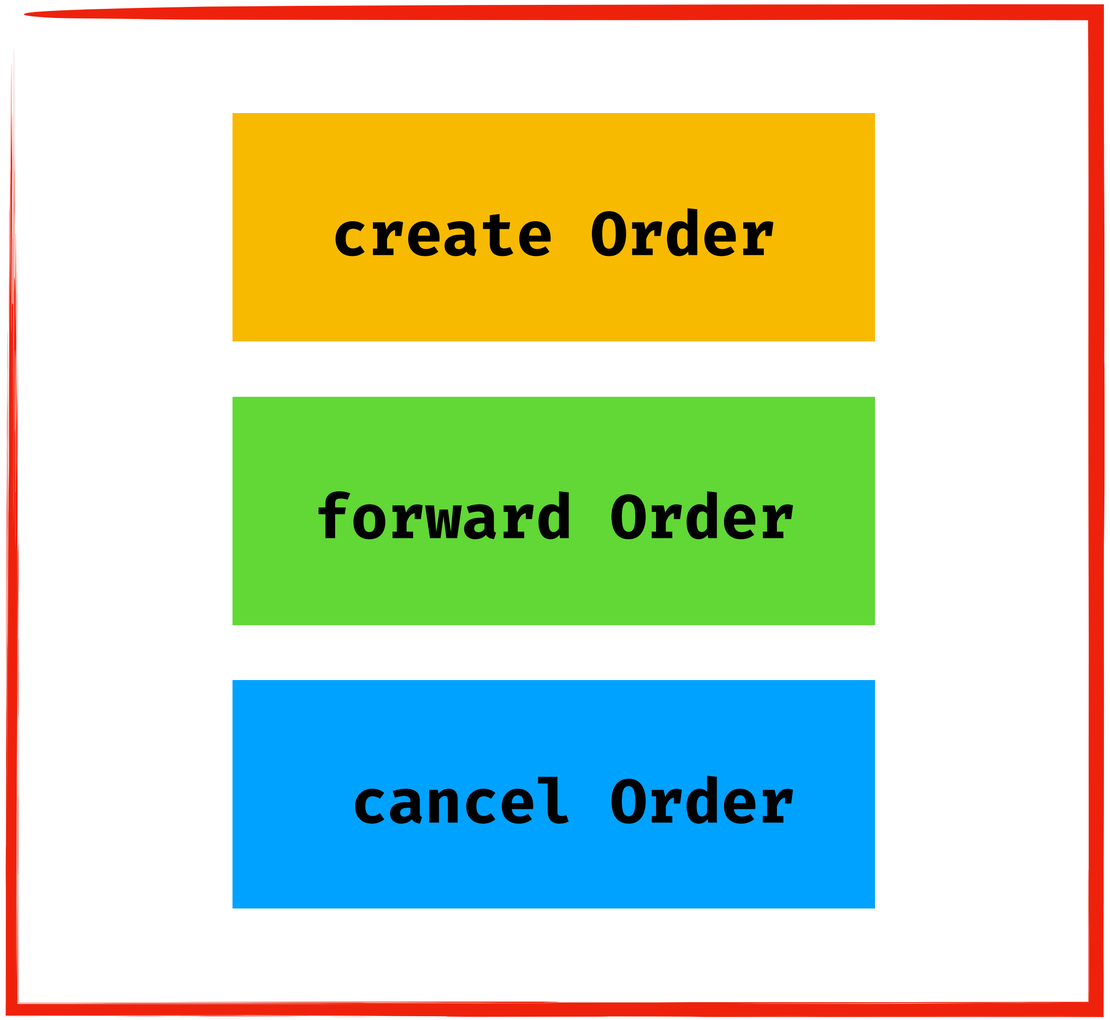
ONE LAMBDA WITH DISPATCH

MULTI LAMBDA - SHARED ZIP

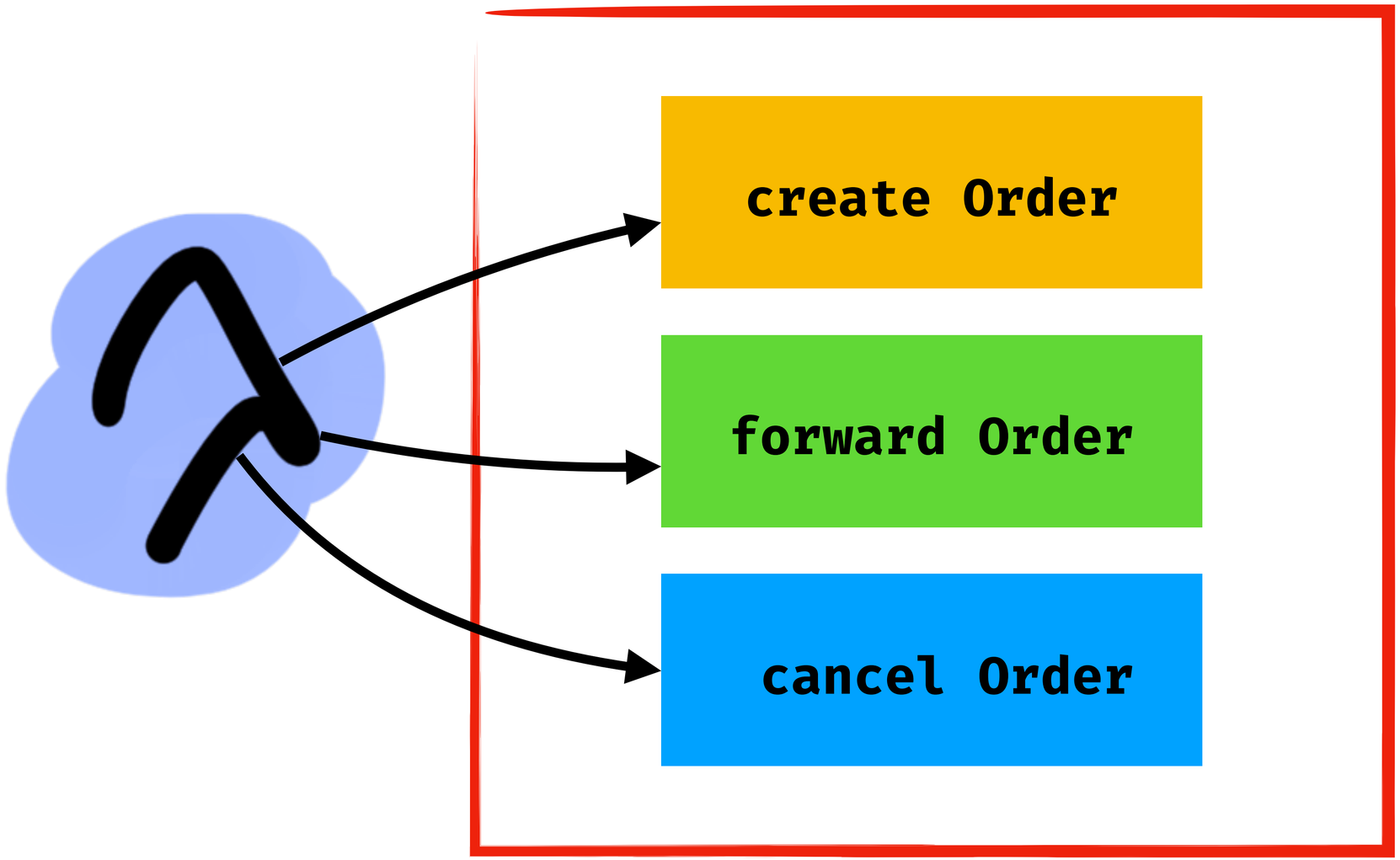
**MULTI LAMBDA - SHARED NOTHING**

# ONE LAMBDA WITH DISPATCH

# Order ZIP



# Order ZIP



EASE OF TRANSITION ✓

FLEXIBILITY ✗

SECURITY ✗

SIZING ✗

DEPLOYMENT ✓

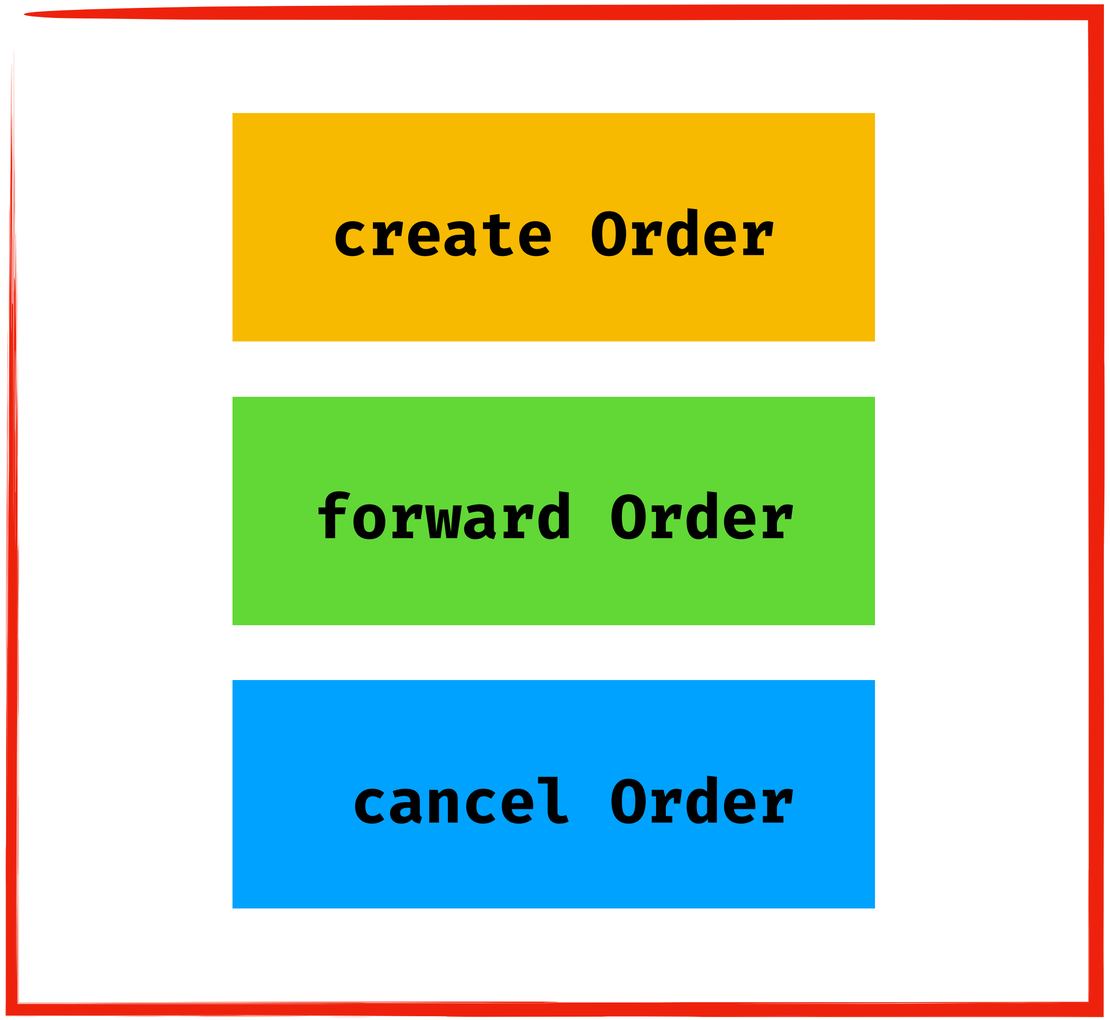
COMPLEXITY ✓

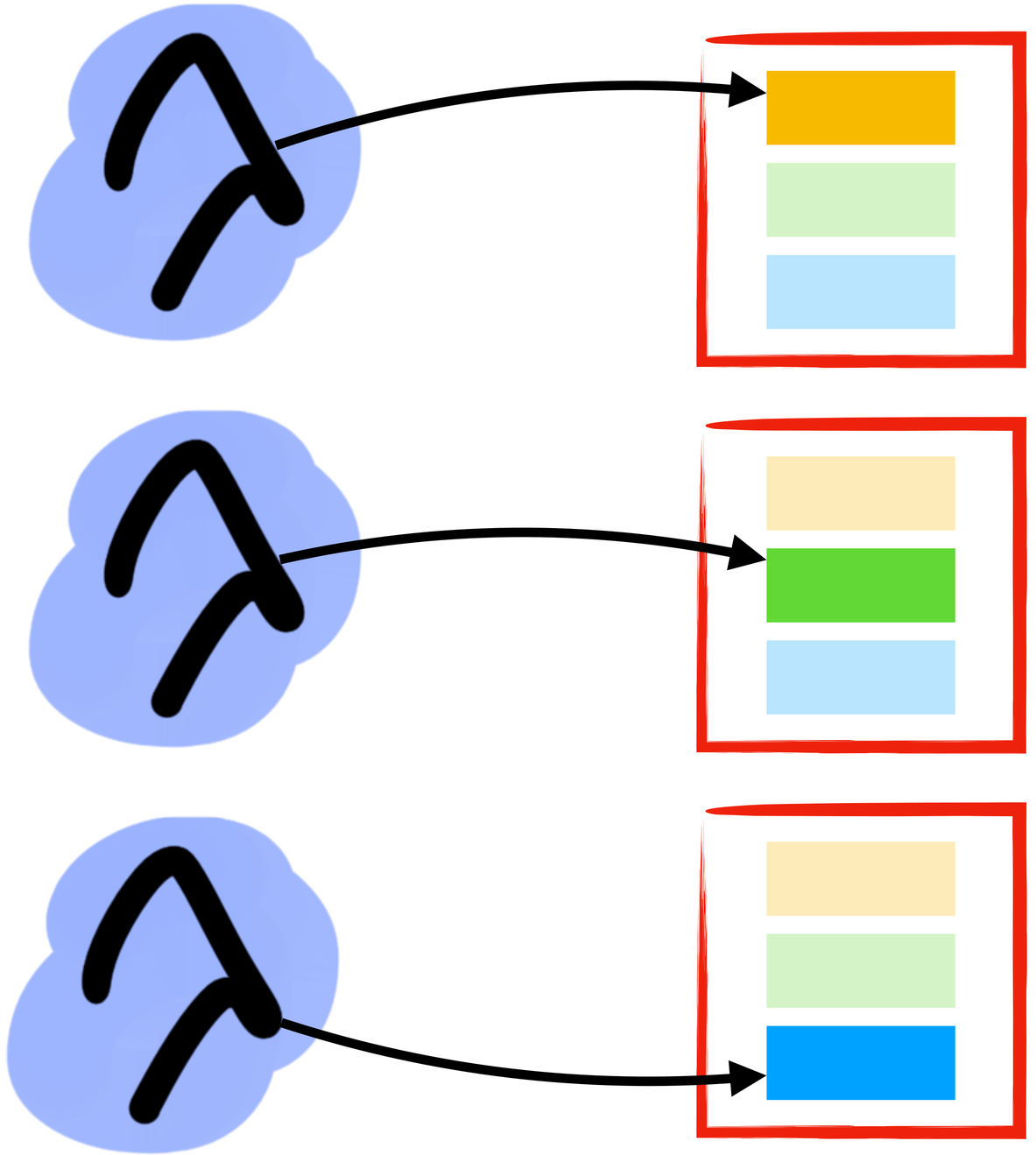
# MULTI LAMBDA

# –

# SHARED ZIP

# Order ZIP





EASE OF TRANSITION 

FLEXIBILITY 

SECURITY 

SIZING 

DEPLOYMENT 

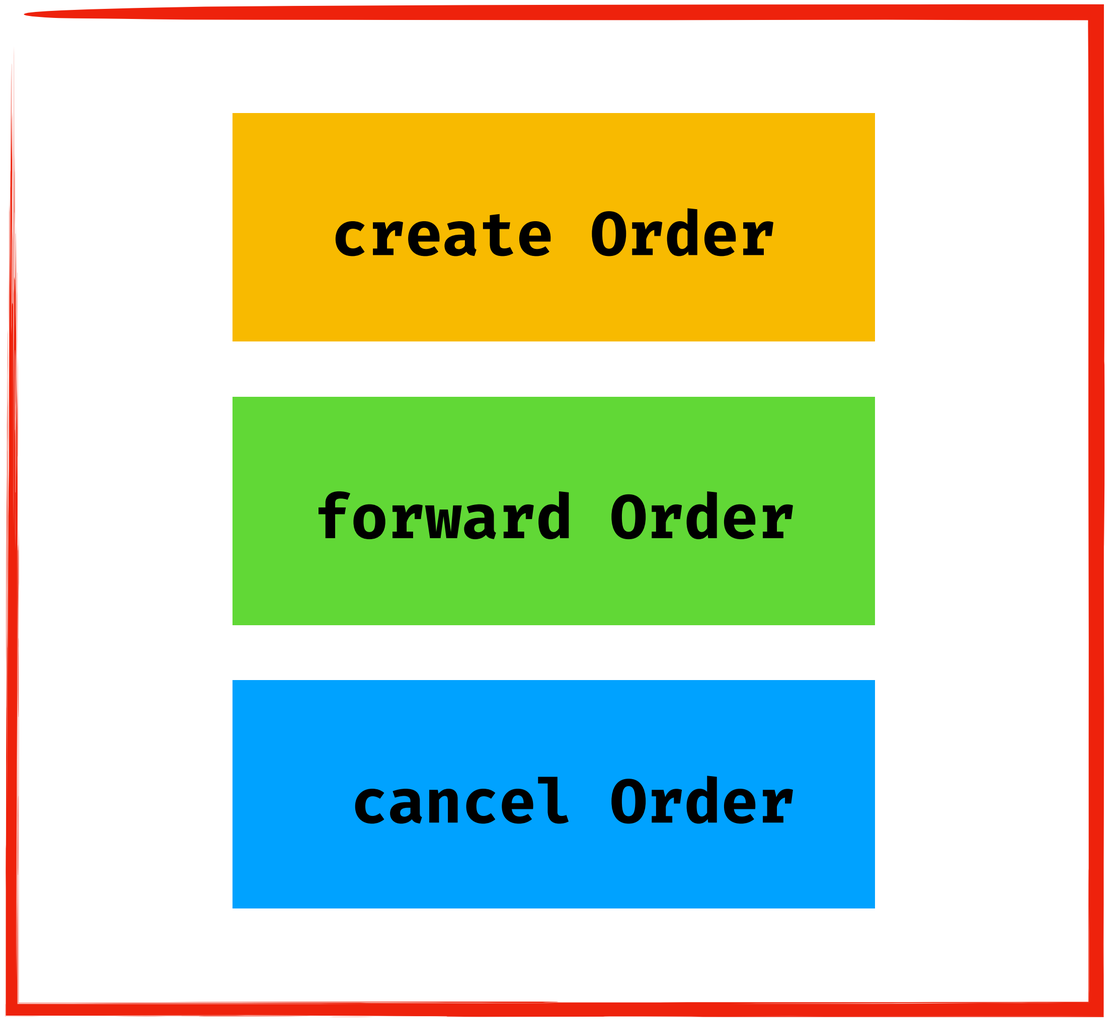
COMPLEXITY 

# MULTI LAMBDA

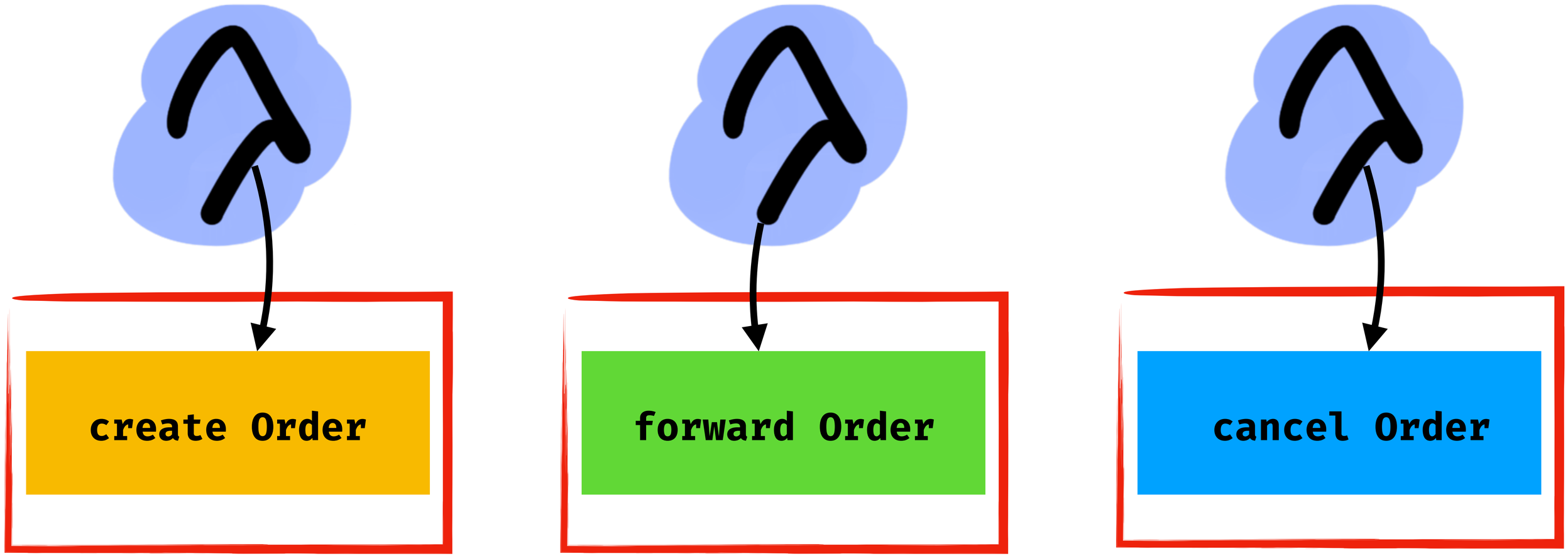
# –

# SHARED NOTHING

# Order ZIP




Create
Order ZIP
create Order
Forward
Order ZIP
forward Order
Cancel
Order ZIP
cancel Order


create Order
forward Order
cancel Order

EASE OF TRANSITION —

FLEXIBILITY ✓

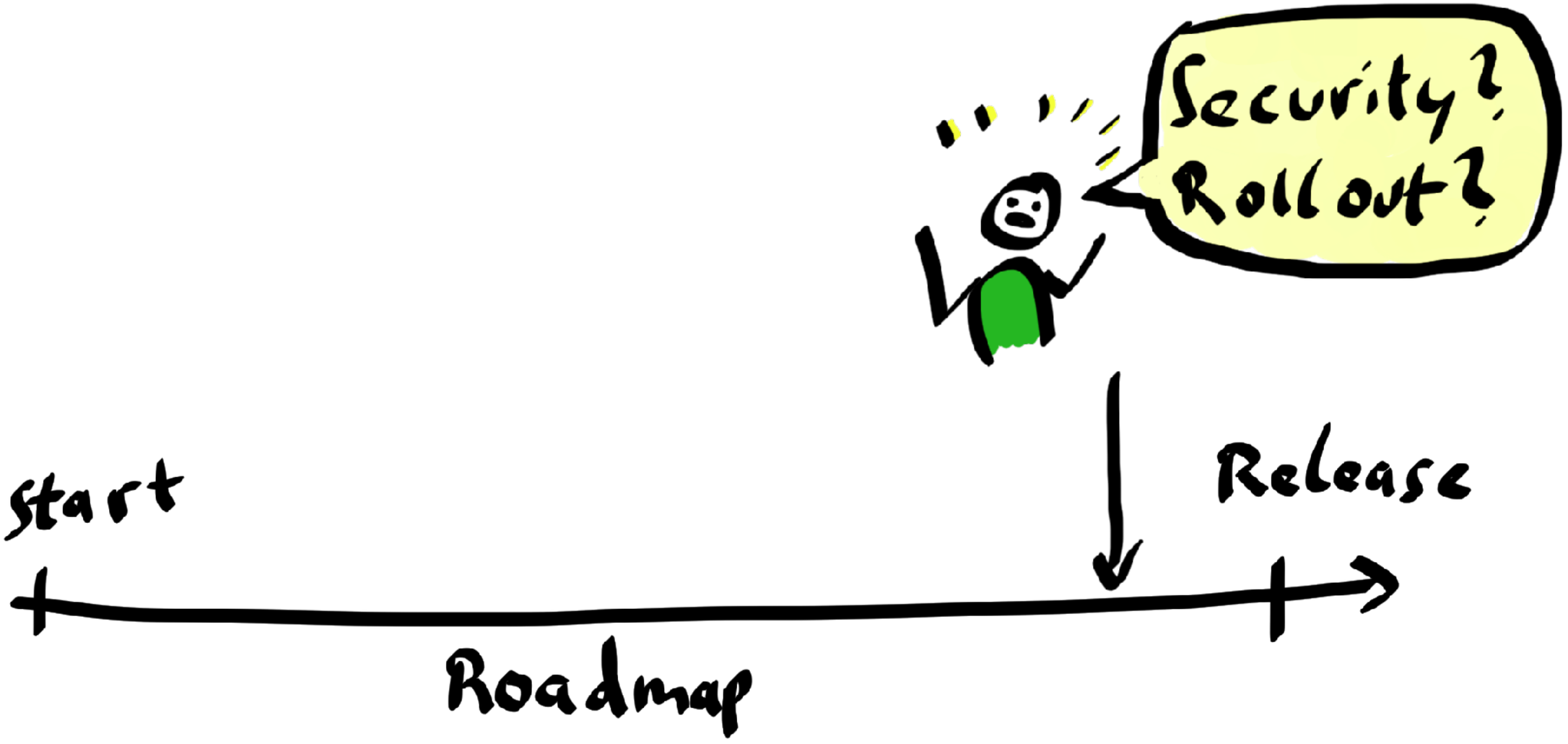
SECURITY ✓

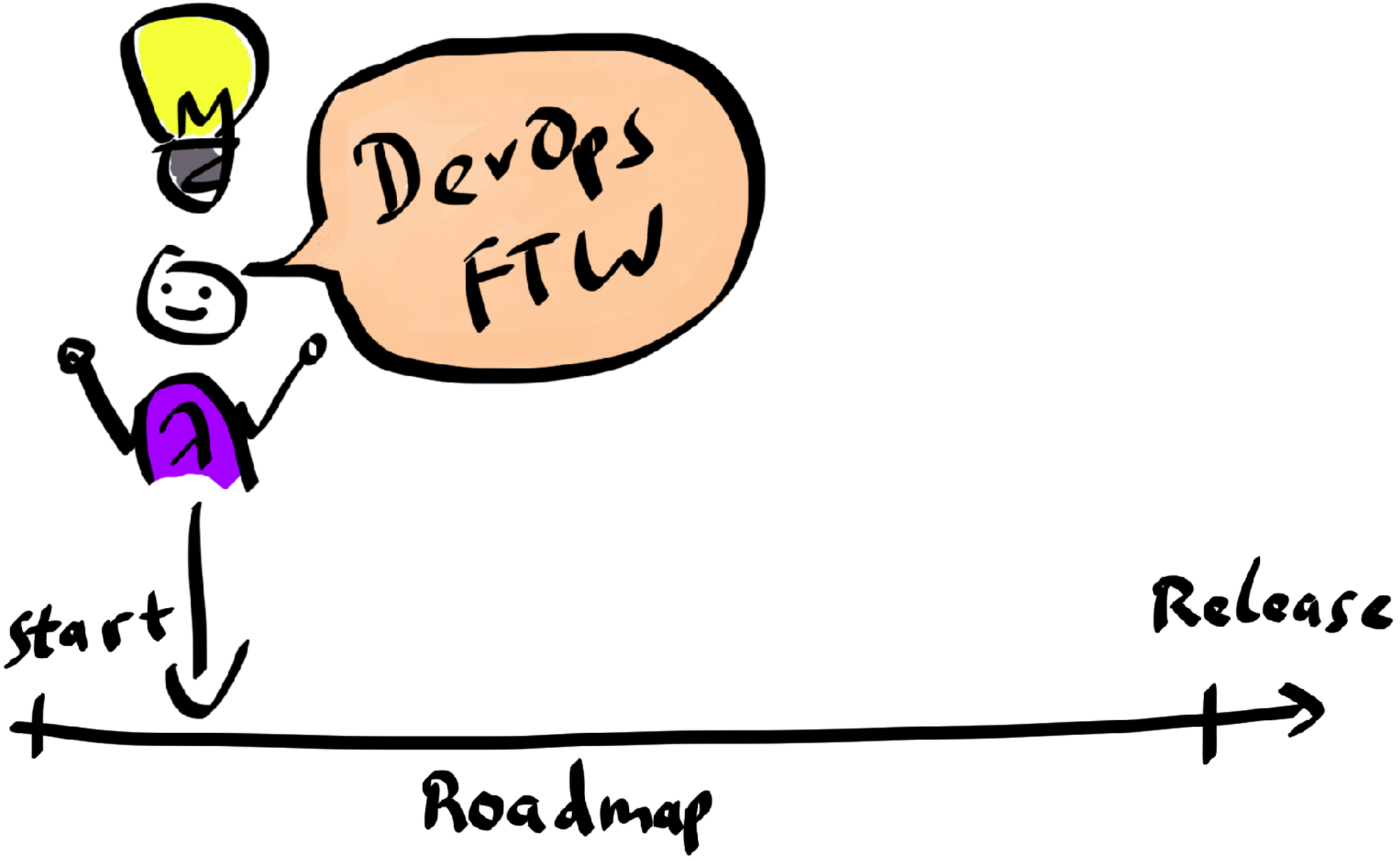
SIZING ✓

DEPLOYMENT ✓

COMPLEXITY —


start
Release
Roadmap


Security?
Roll out?
start
Release
Roadmap


DevOps FTW
start
Release
Roadmap


SUMMARY

# SERVERLESS HYPE TRAIN

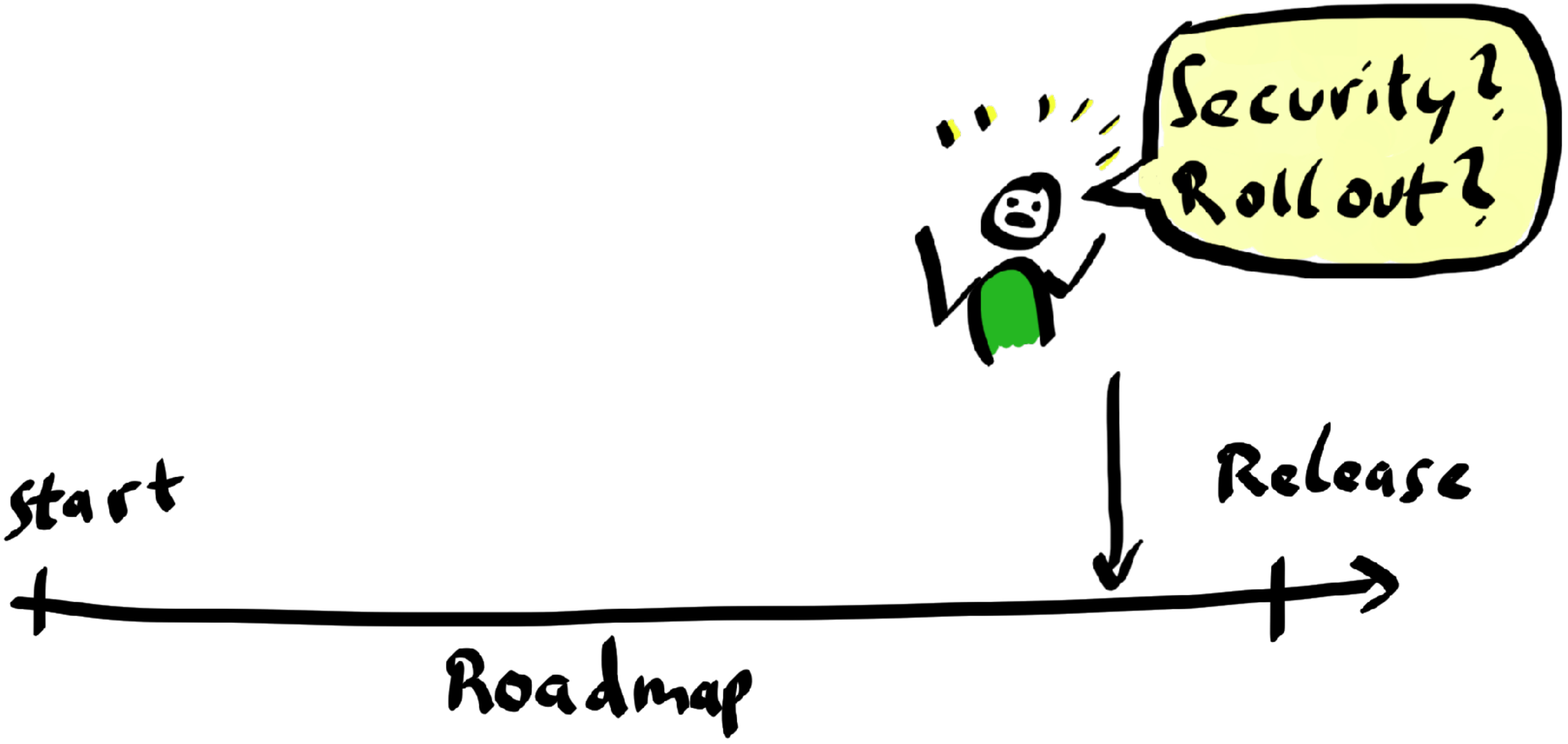
# DESIGNING DISTRIBUTED SYSTEMS IS STILL HARD

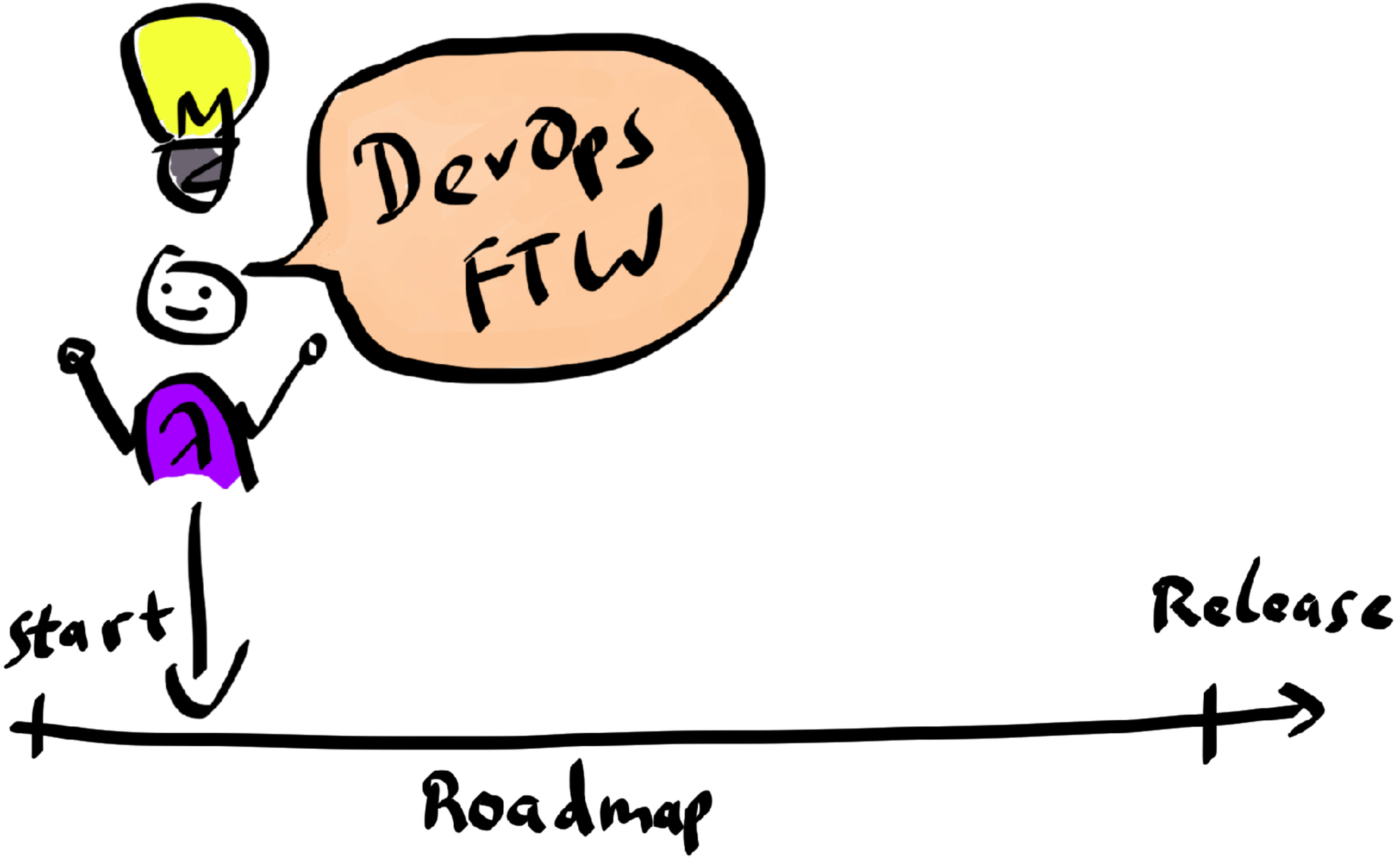
# MOSTLY DIFFERENT CHALLENGES

# YOU NEED A CLOUD-SAVVY OPERATIONS TEAM MEMBER

# DEVOPSSEC DONE RIGHT


start
Release
Roadmap


Security?
Roll out?
start
Release
Roadmap


DevOps FTW
start
Release
Roadmap

# TOOLING IS STILL EVOLVING

# NOT A SILVER BULLET

# SOMETIMES A SIMPLE VM IS ENOUGH

# SERVERLESS

# LESS SERVERS THAT WE NEED TO TAKE CARE OF


# THANK YOU!

## FEEDBACK? COMMENTS?
## QUESTIONS?

## @KOENIGHOTZE