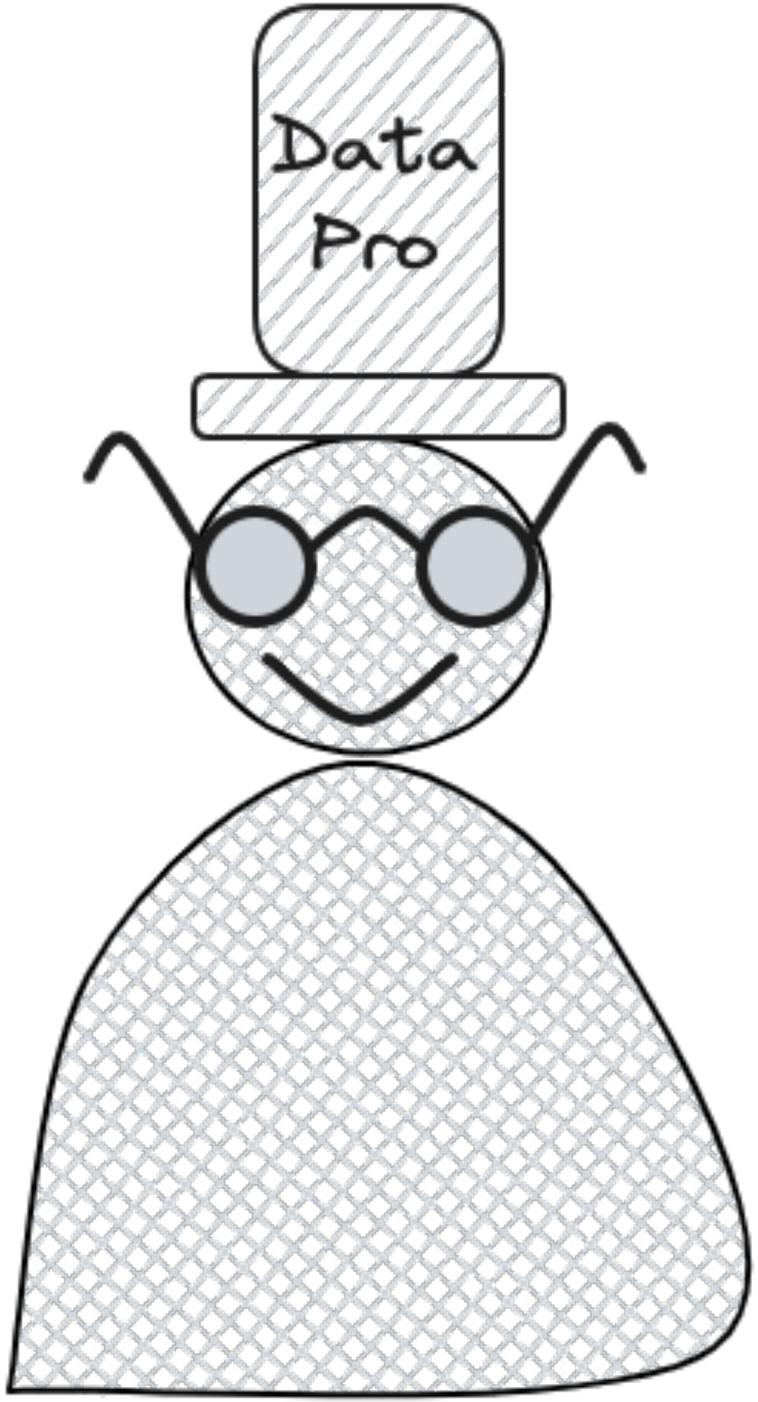
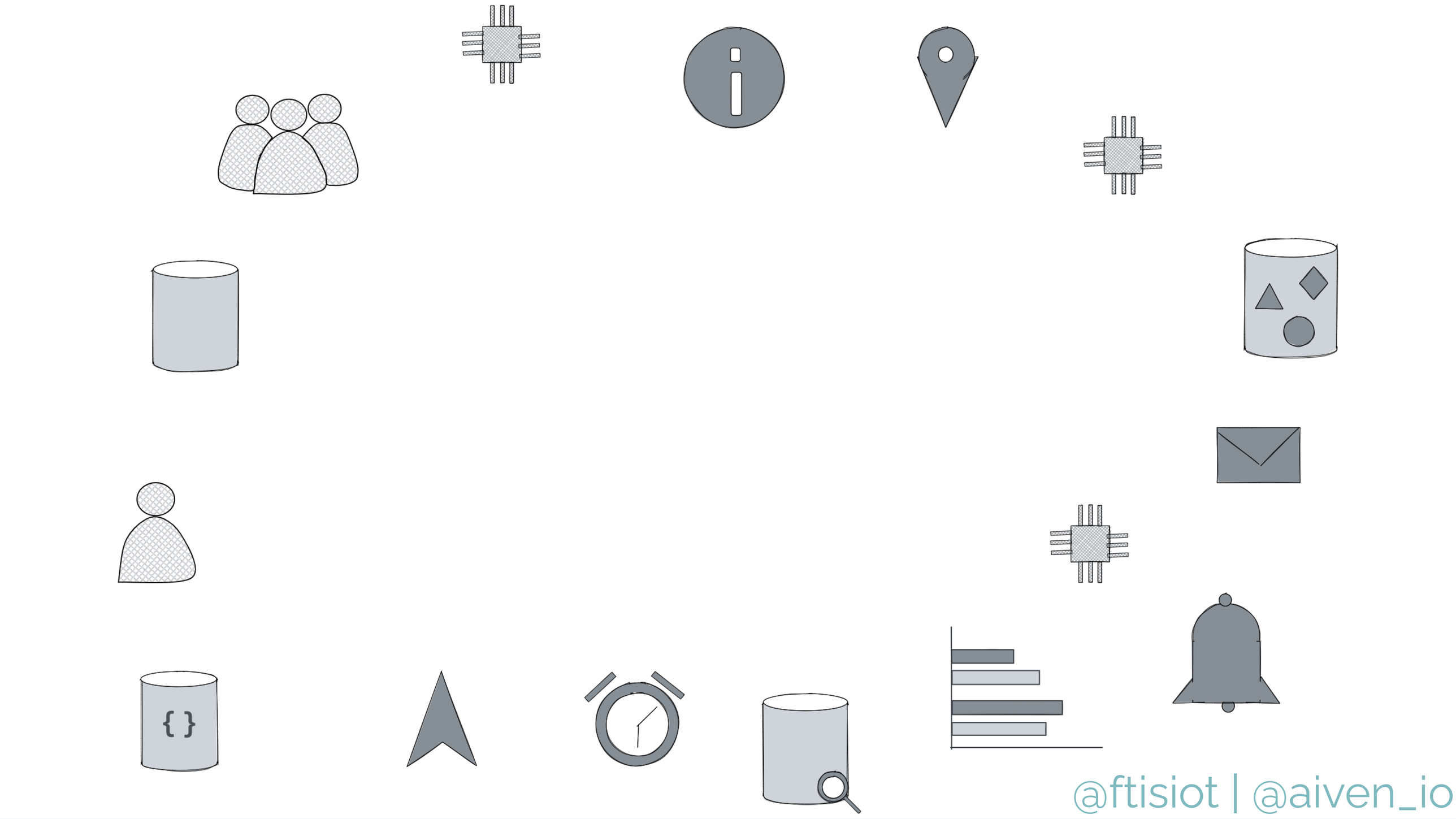
aiven

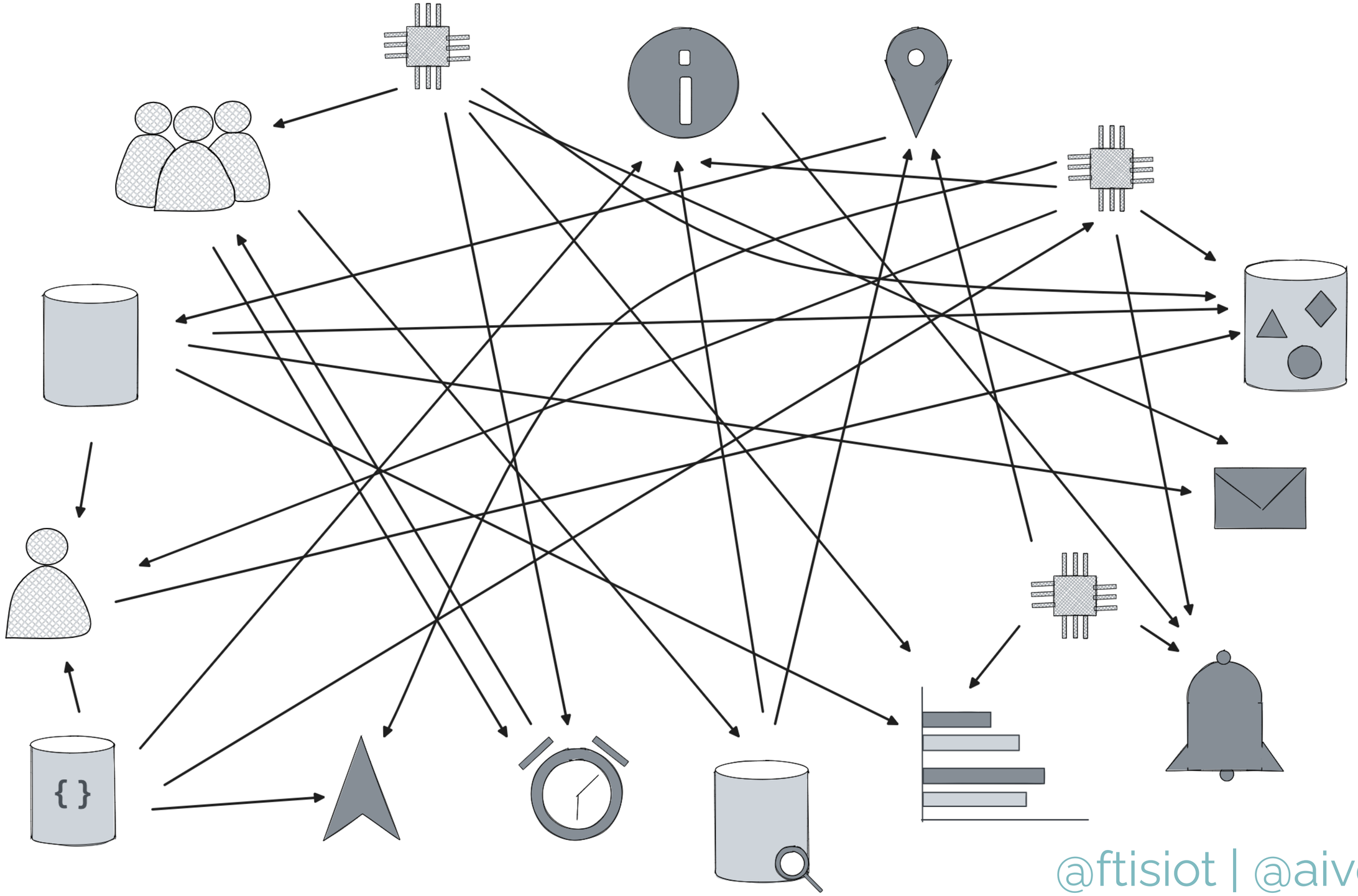
Attacking (and defending) Apache Kafka

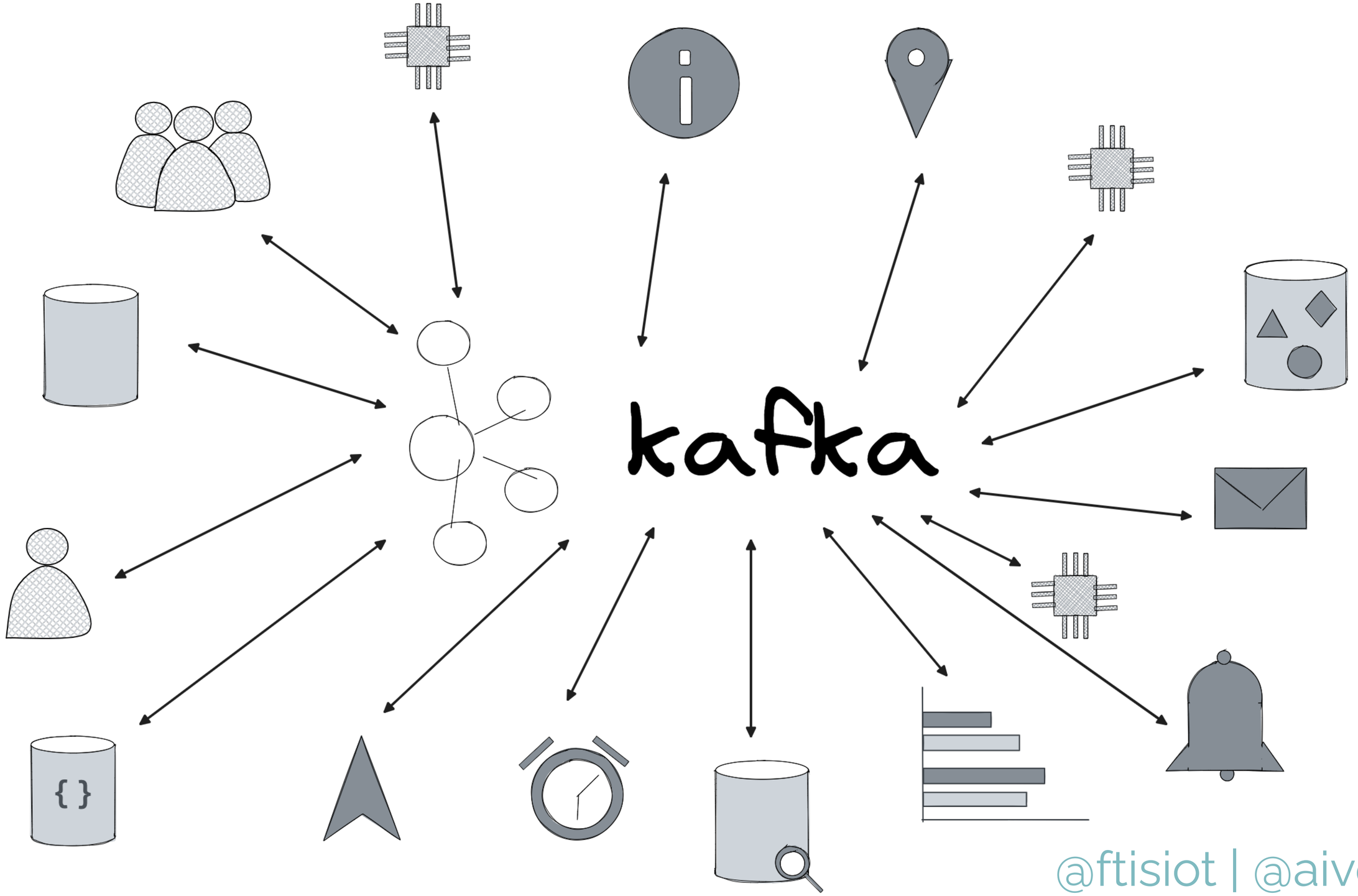
Francesco Tisiot - Staff Developer Advocate

@ftisiot

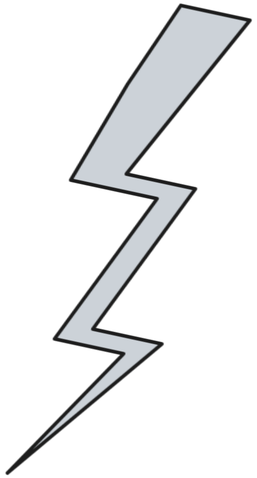

Data
Pro



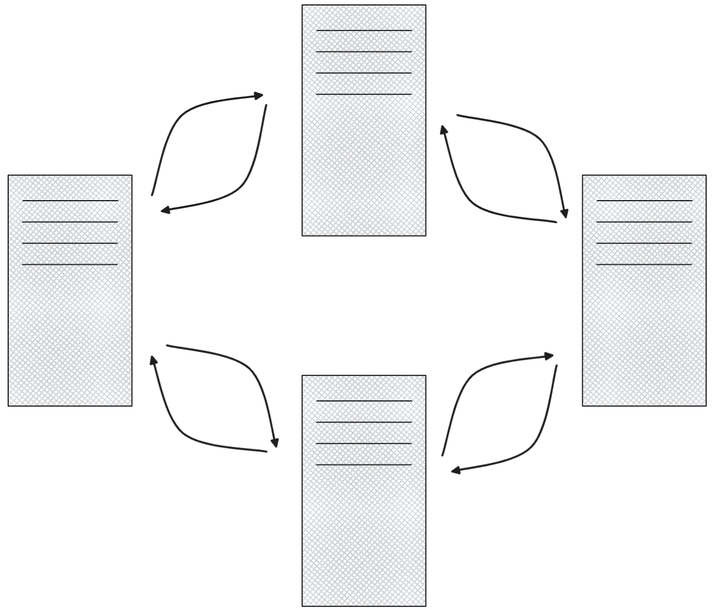



kafka
{ }

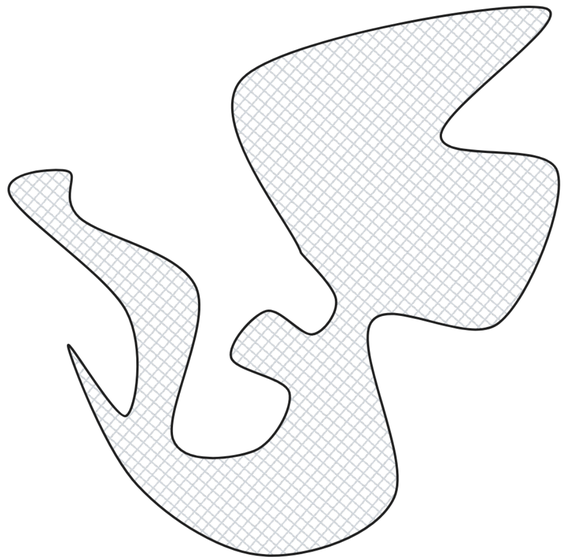
Streaming



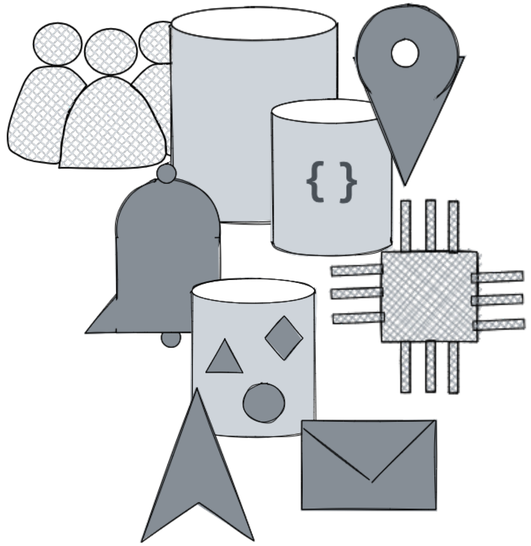
Distributed

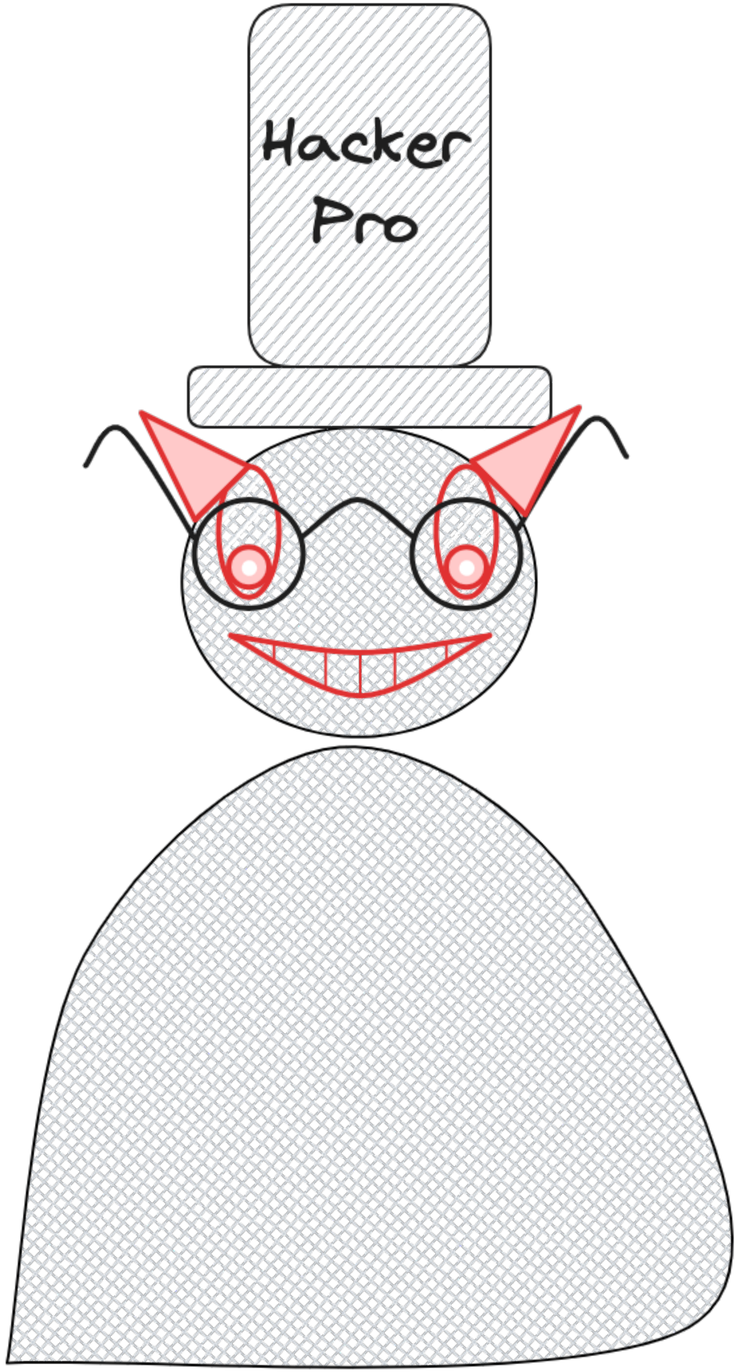


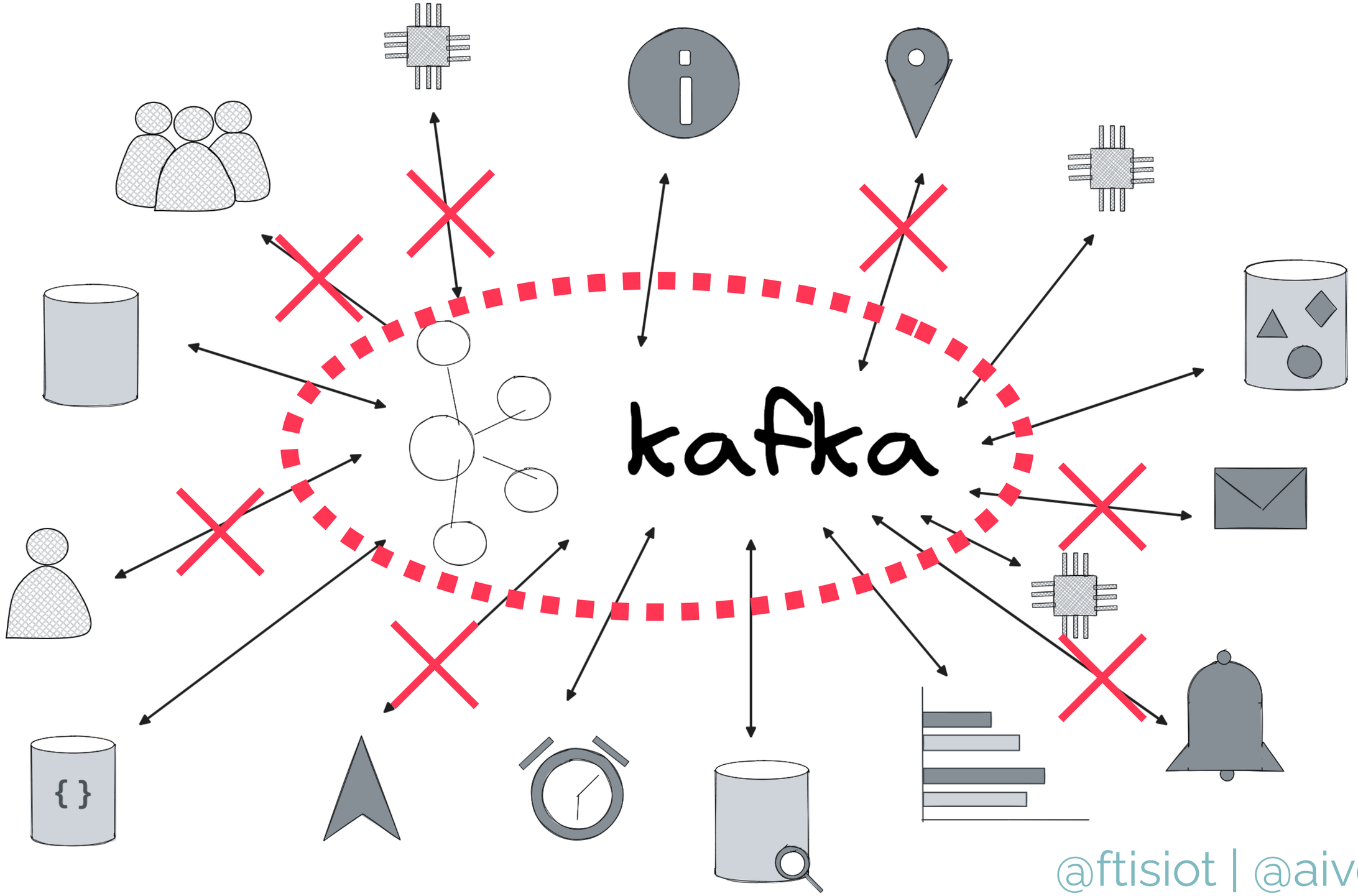
Flexible

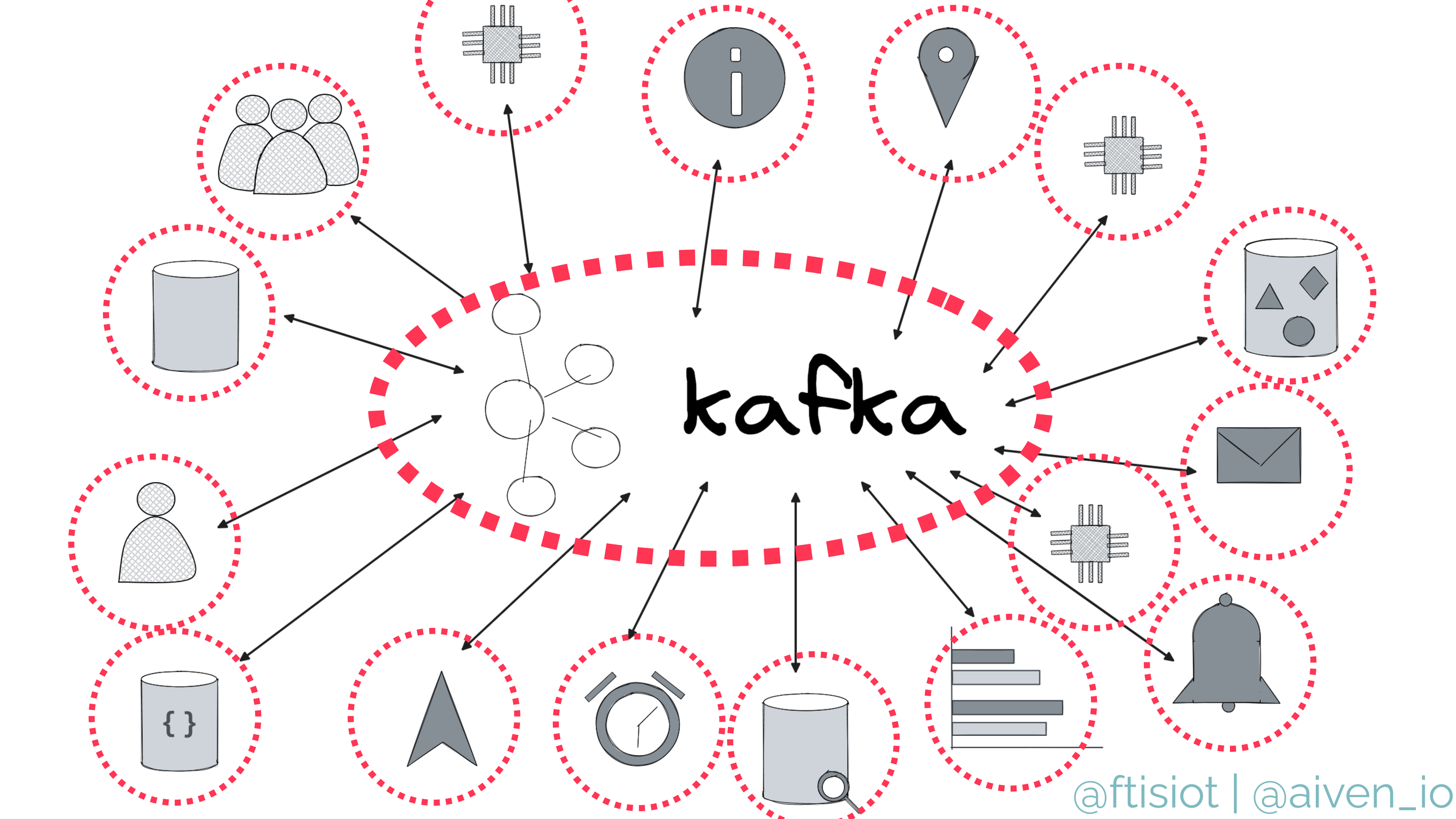


Integratable




Hacker
Pro


kafka
{ }


kafka
{ }

Streaming

Fast Damage
Time to response

Distributed

Access/Damages
one node
=
disrupt the entire
cluster

Flexible

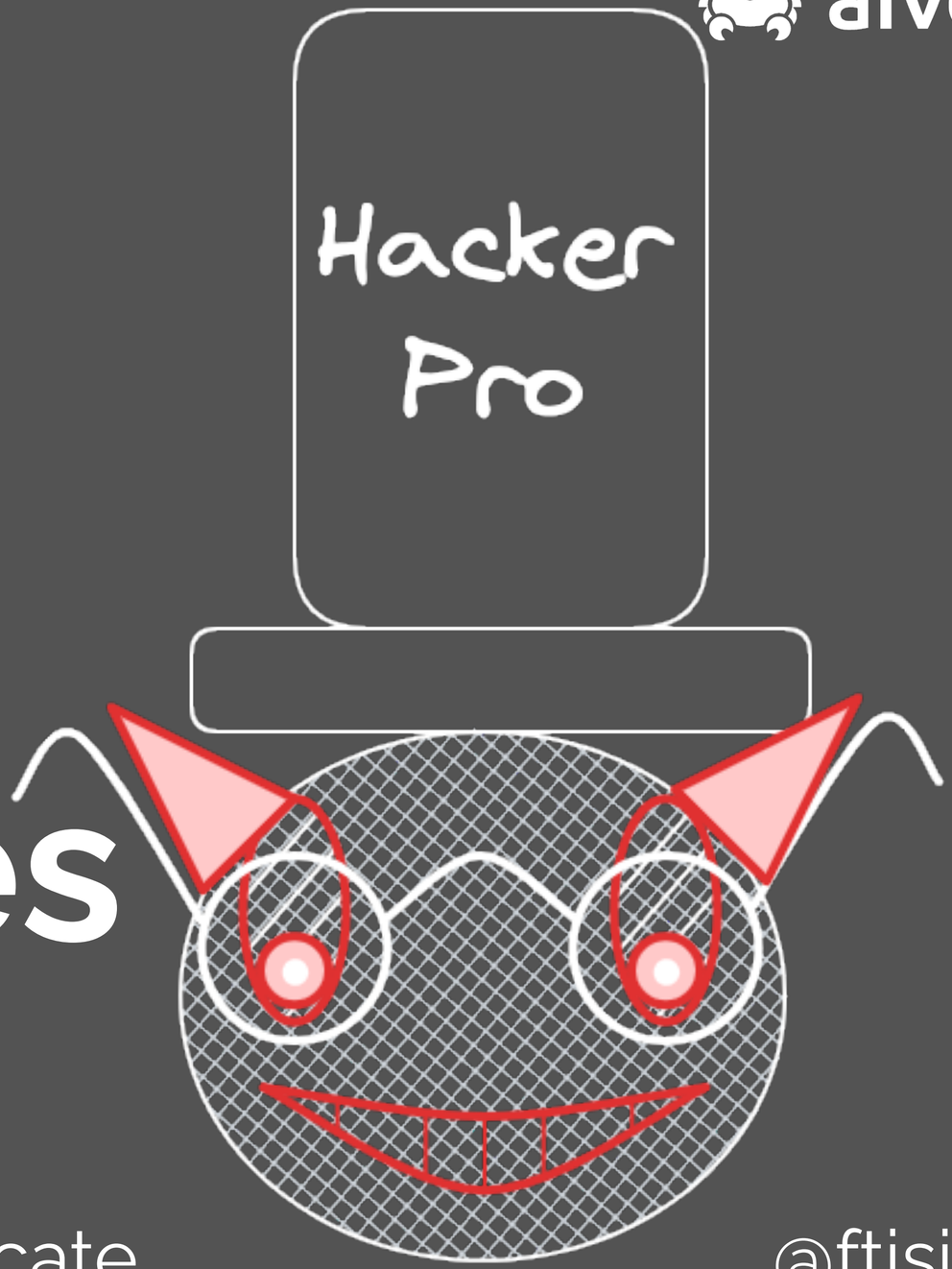
Hard to monitor

Integratable

Stop of workflows
Credentials of Source/Sink systems

aiven

Apache Kafka from the attacker lenses



Francesco Tisiot - Staff Developer Advocate

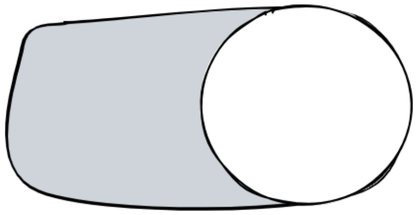
@ftisiot

aiven

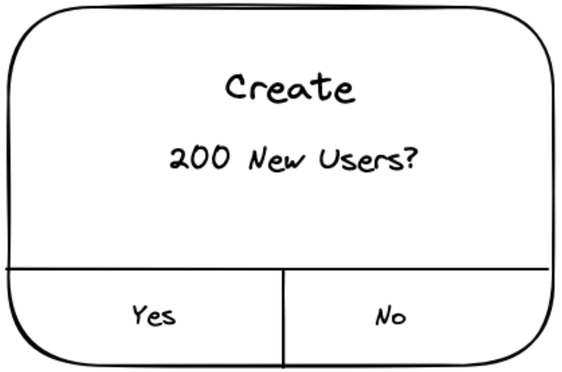
Intent

Francesco Tisiot - Staff Developer Advocate

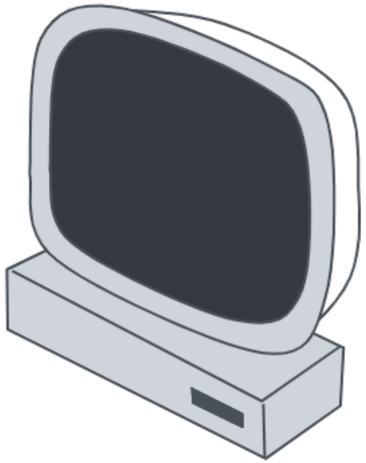
@ftisiot



Abuse In Place



Abuse of Business Logic



Abuse post Exploitation

Crypto Mining

CC phishing

Monetisation

Use for FREE

DDoS Zombies

Hacking Platforms

Weaponisation

Storing Artefacts

Impersonation

Mis/Disinformation

Disinformation campaigns

Extorsion

Cyberbullying

Victimisation

Scams

Vandalism

Disruption

Cause chaos

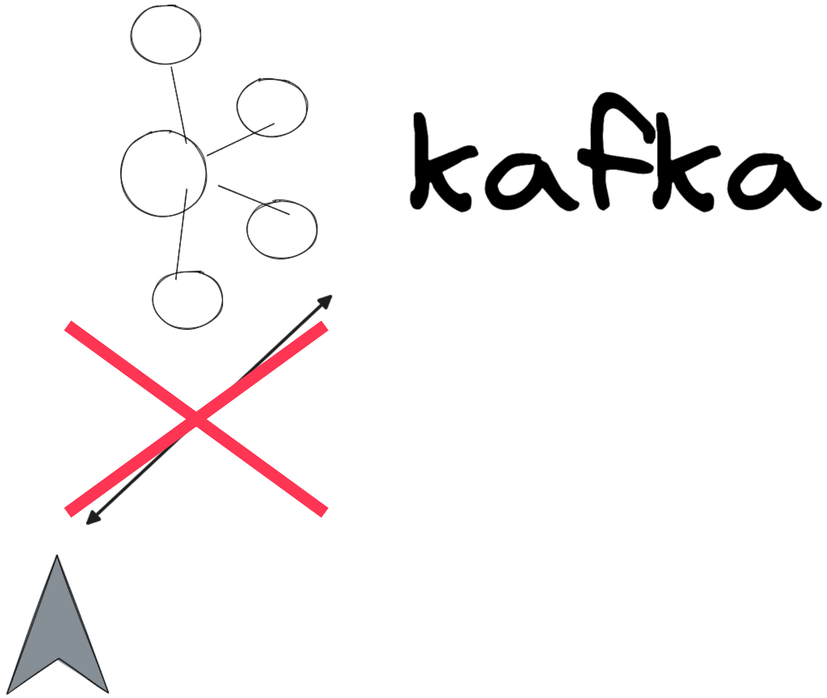
Swap reputation

Achieve popularity

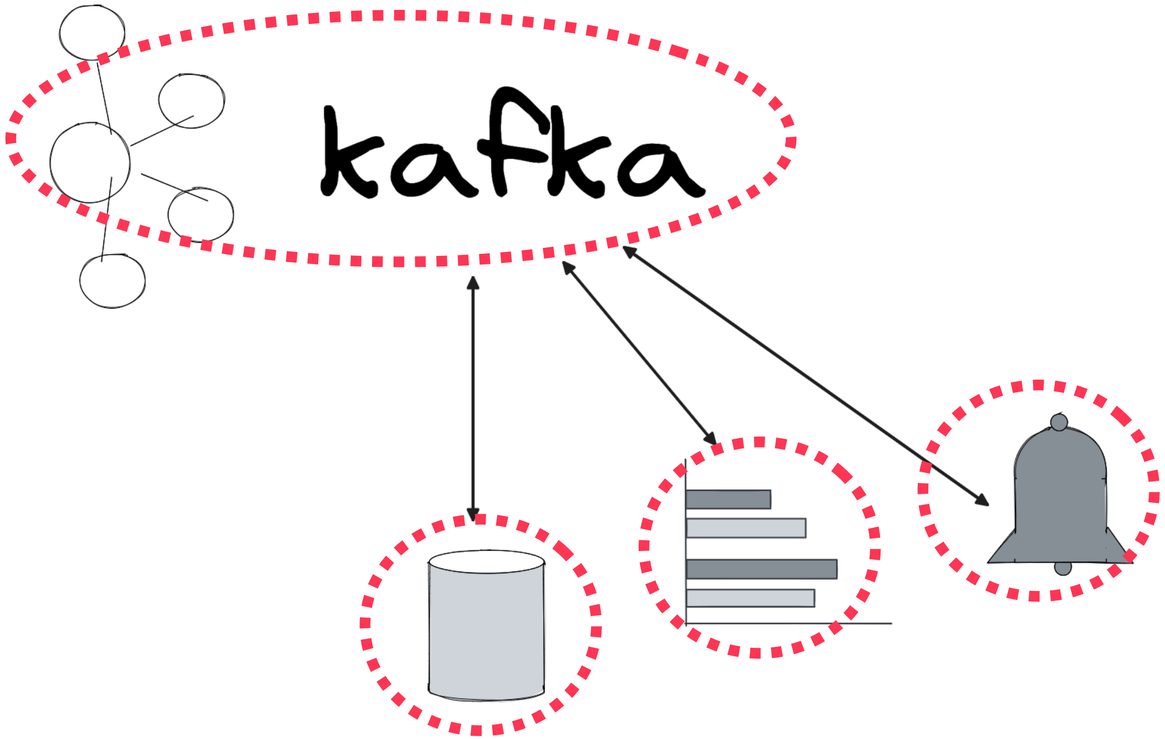
Reputation Manipulation

Bragging rights

Service Disruption



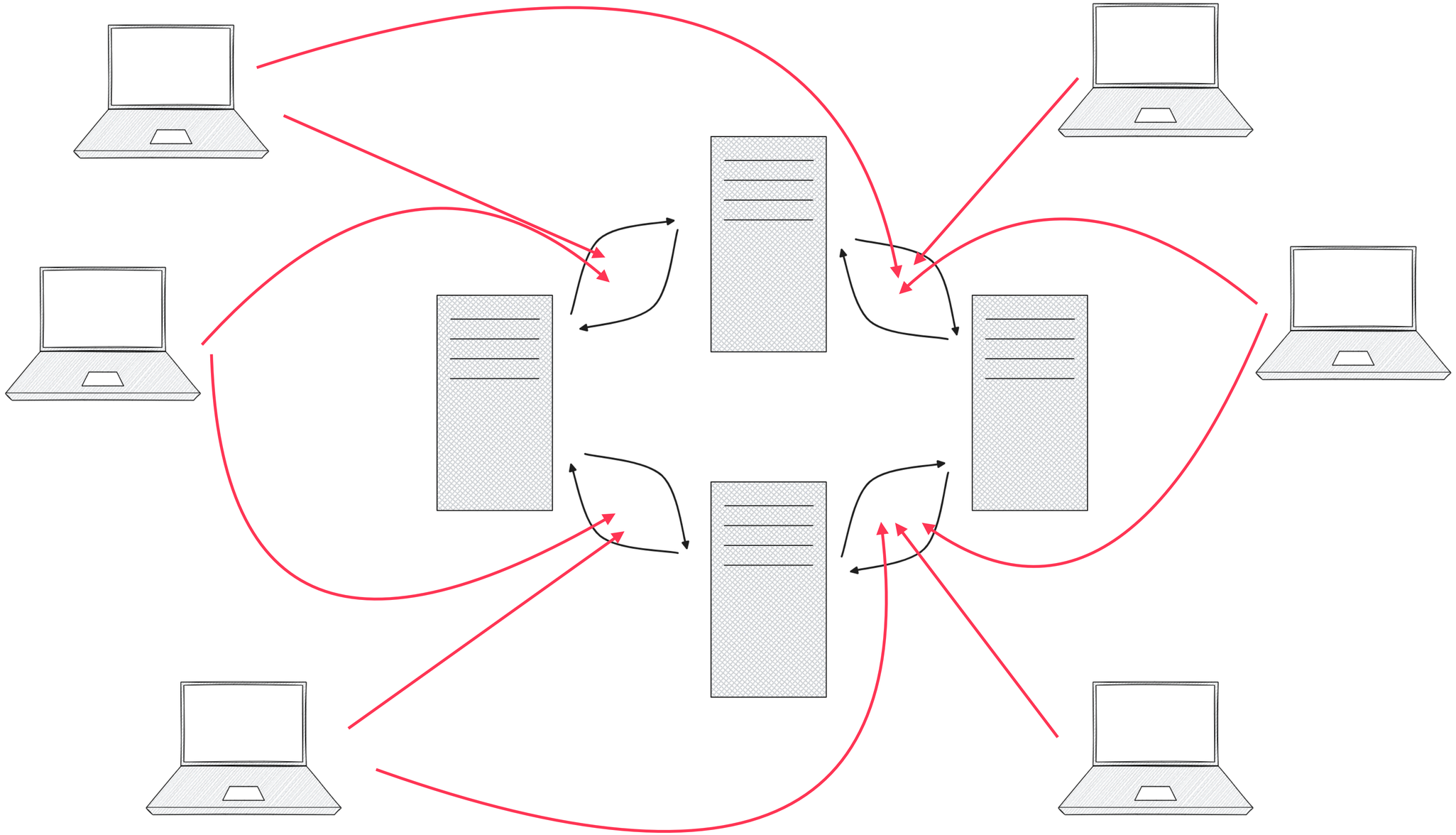
Data Alteration/Stealing



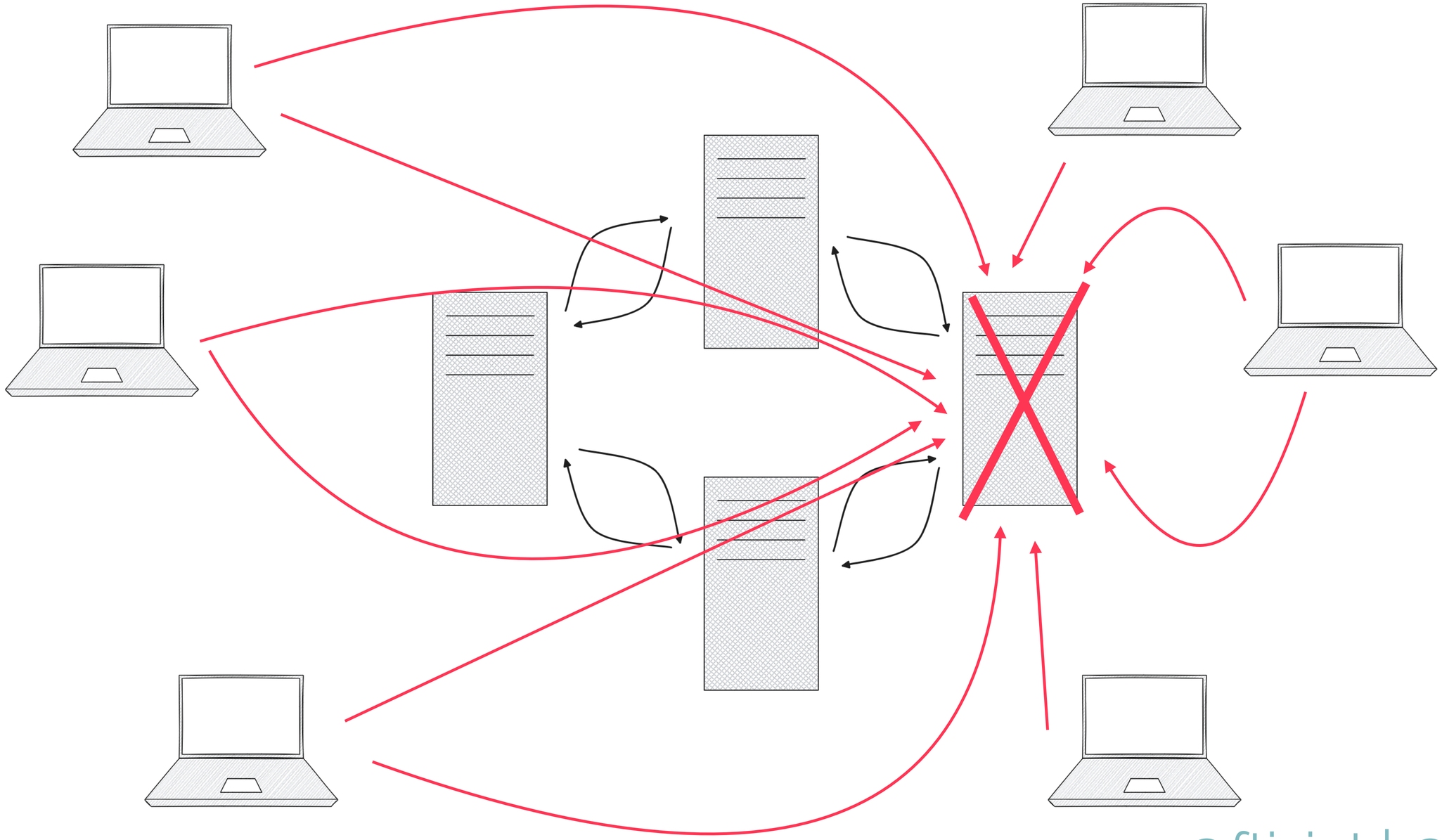
aiven

Yes, but How?

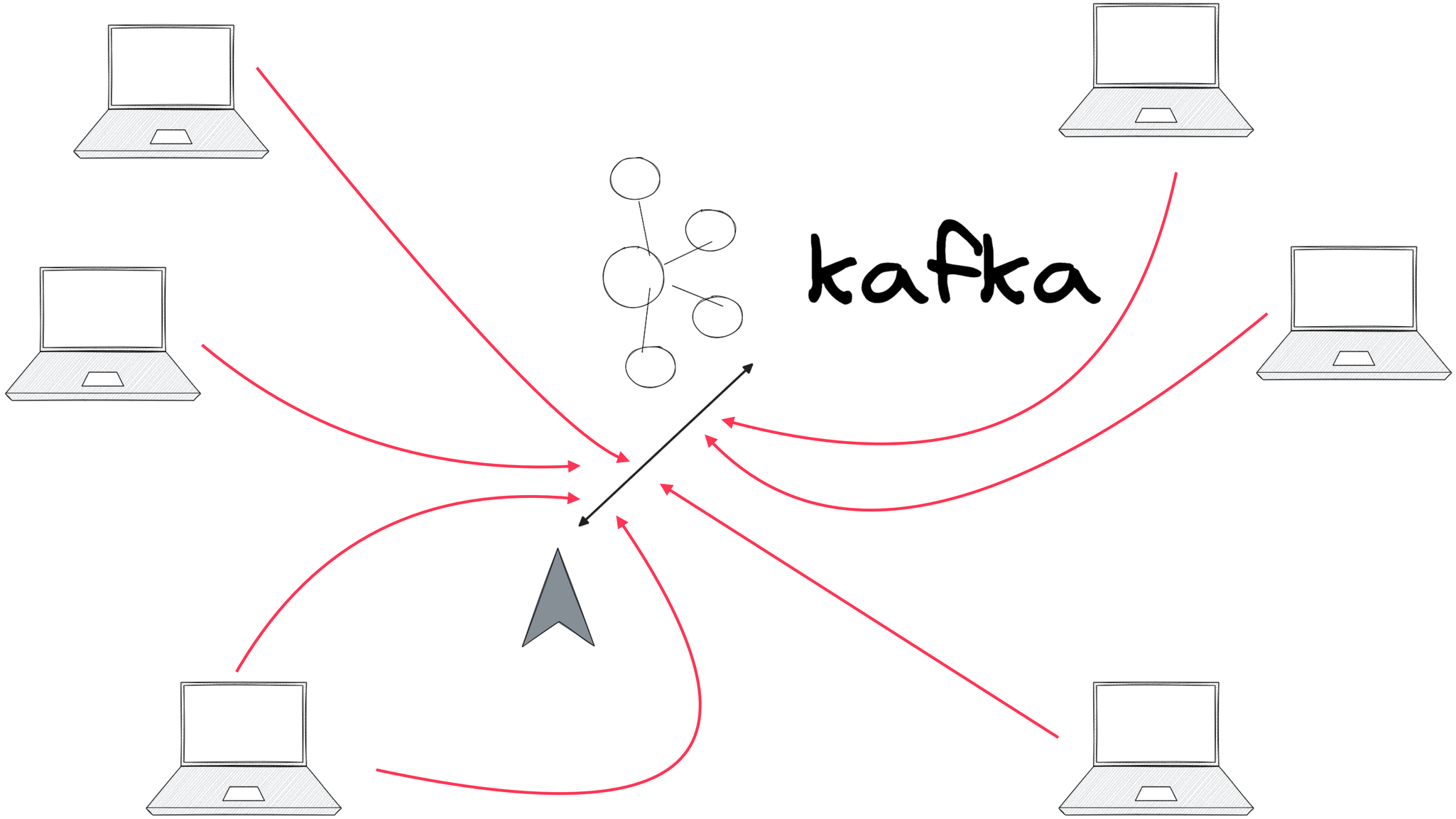
Network DDoS



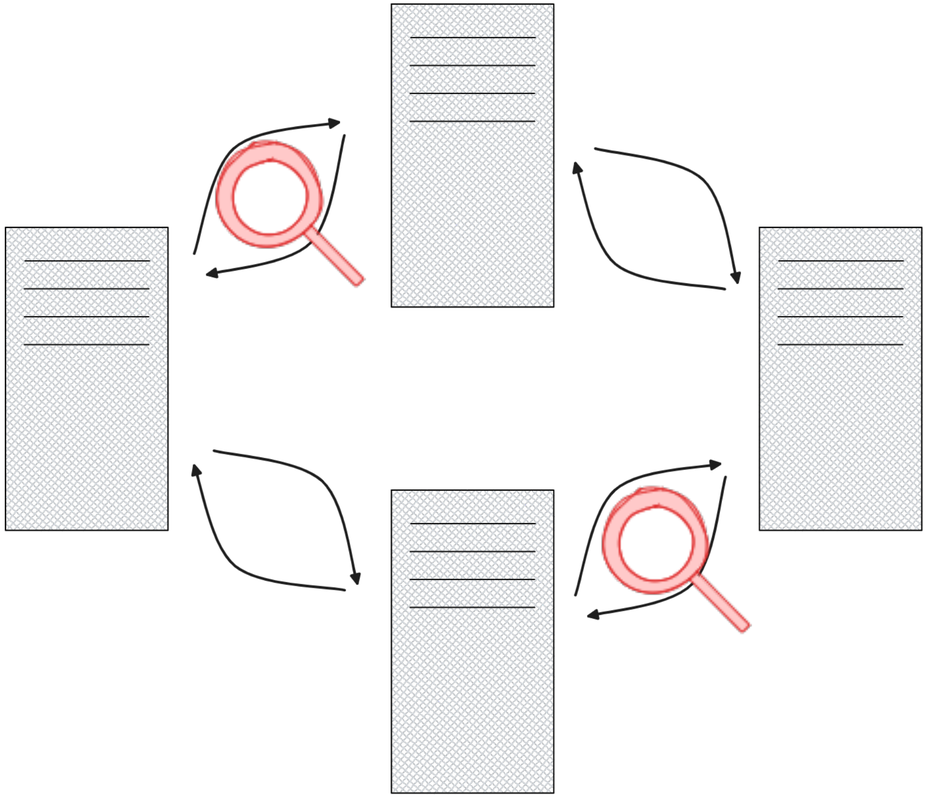
Node DDoS

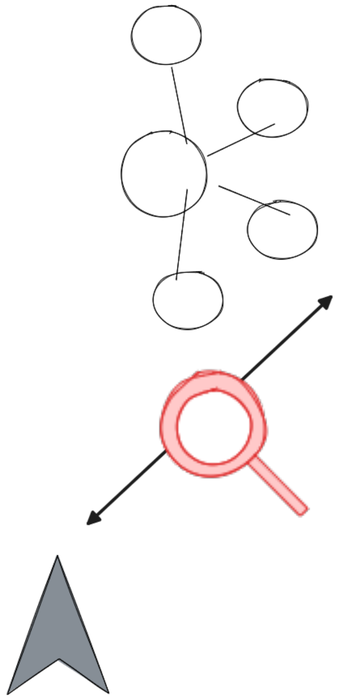


Network DDoS



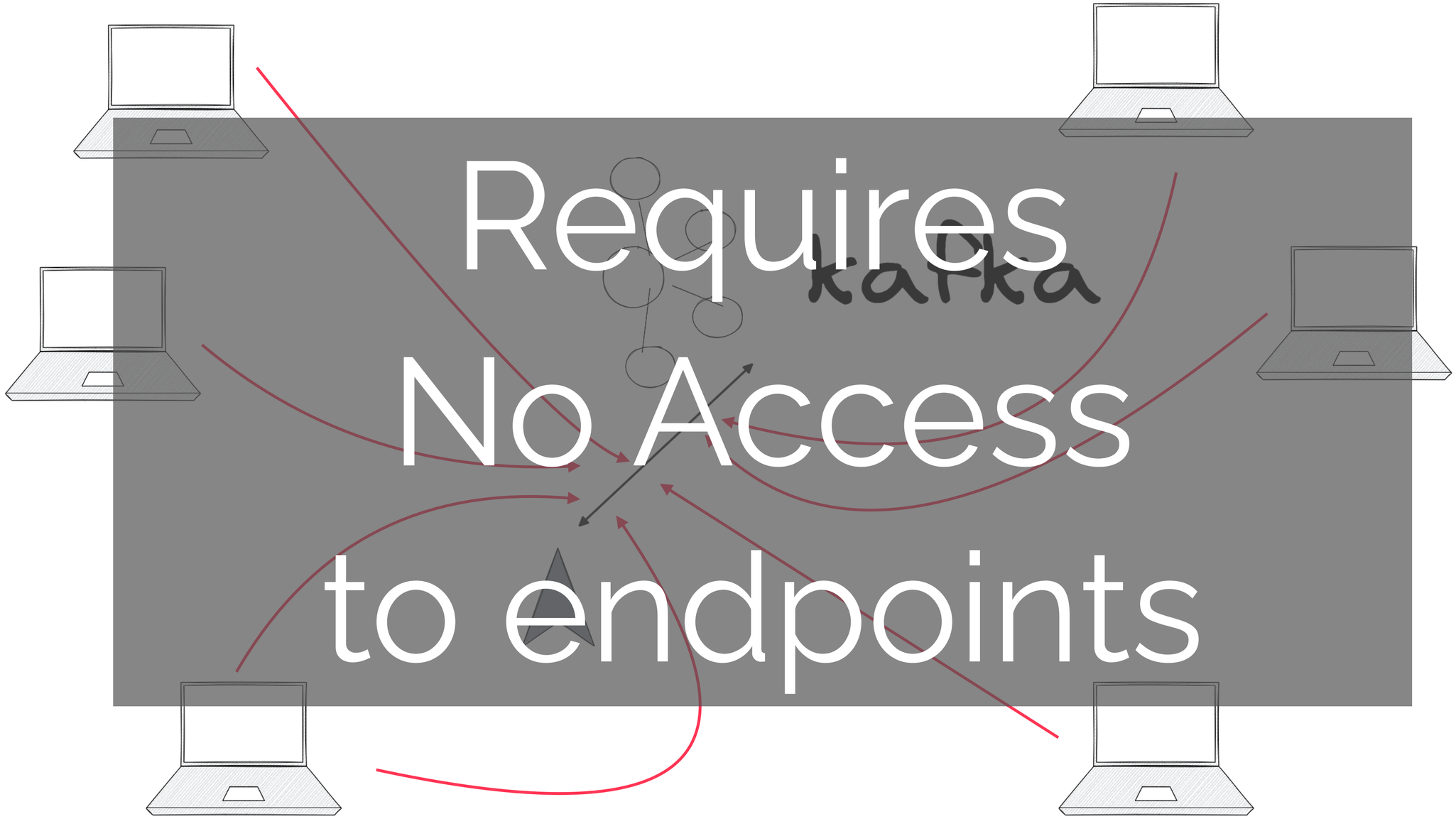
Network Sniffing





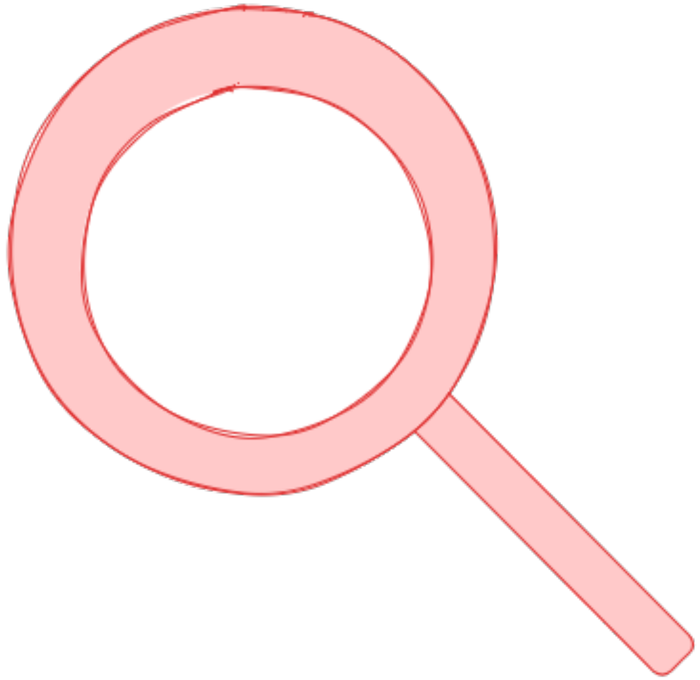
kafka

Network DDoS/Sniffing



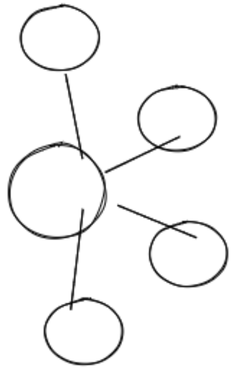
Requires
No Access
to endpoints

Service Disruption

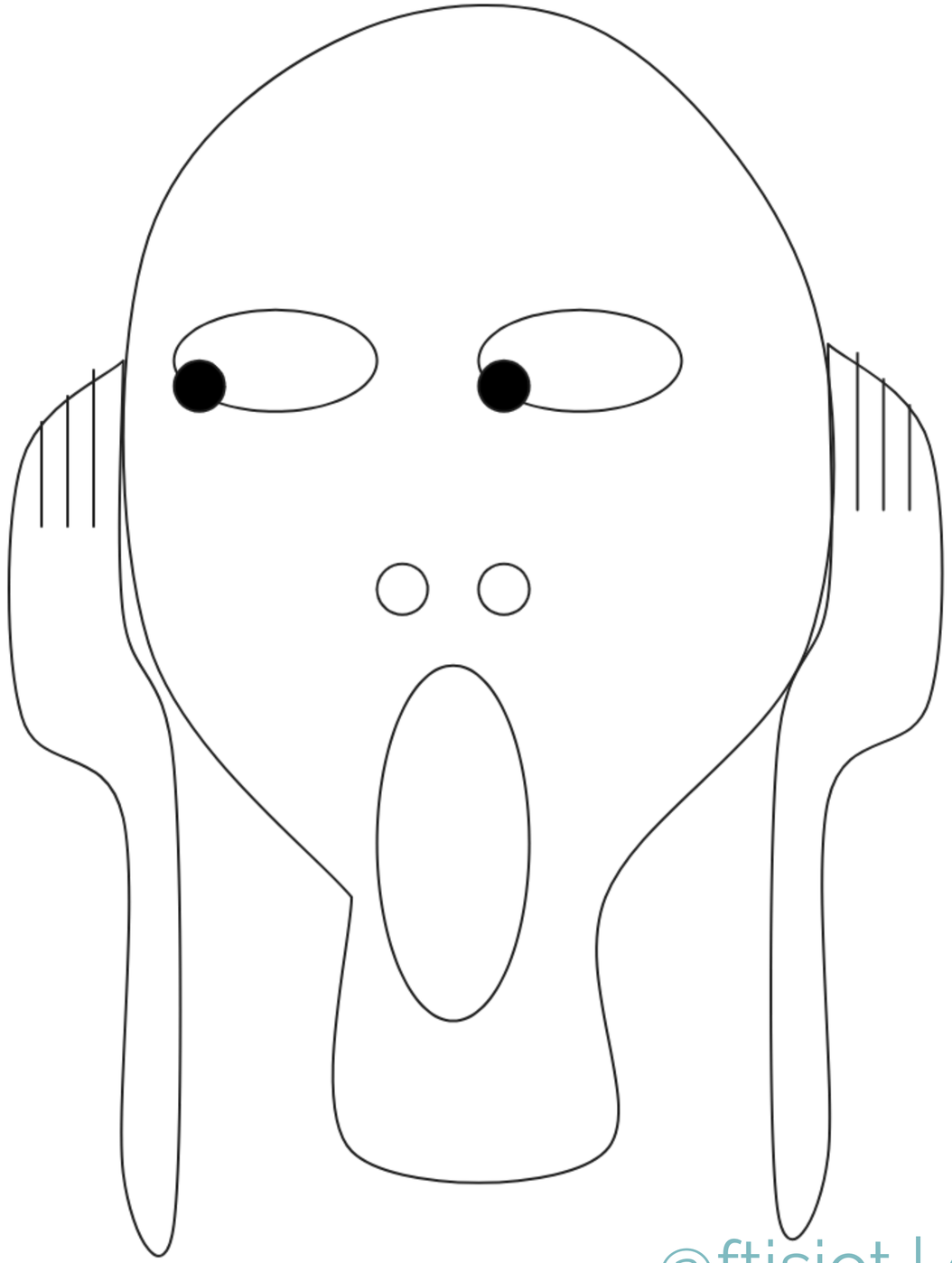


Data

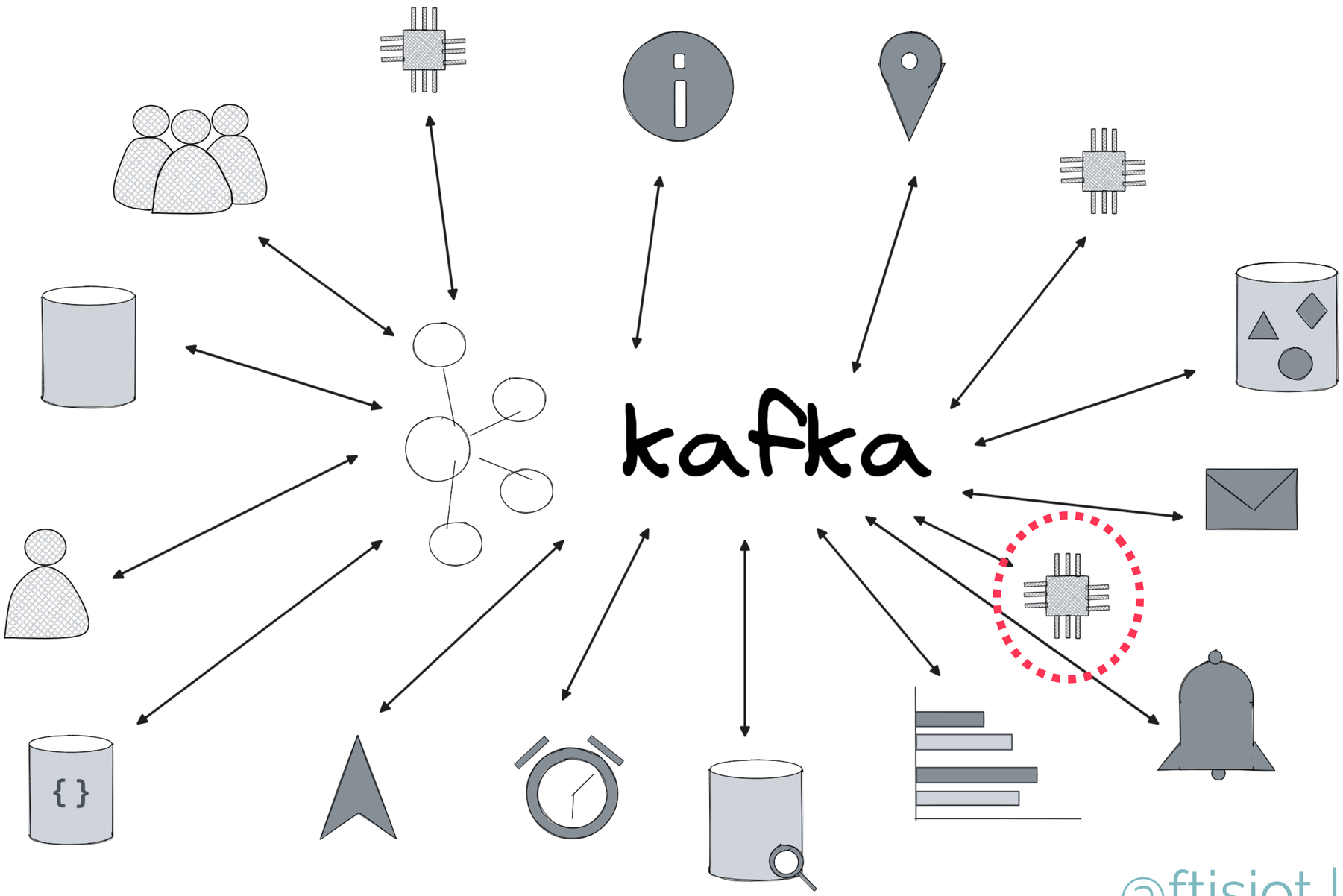
Credentials



kafka



Gain Access to a Producer



```
{
        "name": "Francesco",
        "amount": "-100$"
}
```

Breaking the soft laws

```
{
    "name": "Myverylongnamethatistoolongformydownstreamdatabase.....",
    "amount": "-100$"
}
```

Generating Cascading Effects

```
{
        "name": "Francesco",
        "amount": "'; DROP TABLE USERS;"
}
```

"Cancelling" events

```
{
    "name": "Francesco",
    "amount": "-100$"
}
```

```
{
    "name": "Francesco",
    "amount": "100$"
}
```

"Cancelling" events...slowly


```
{
    "name": "Francesco",
    "amount": "-100$"
}
```

```
{
    "name": "Francesco",
    "amount": "5$"
}
```

```
{
    "name": "Francesco",
    "amount": "2$"
}
```

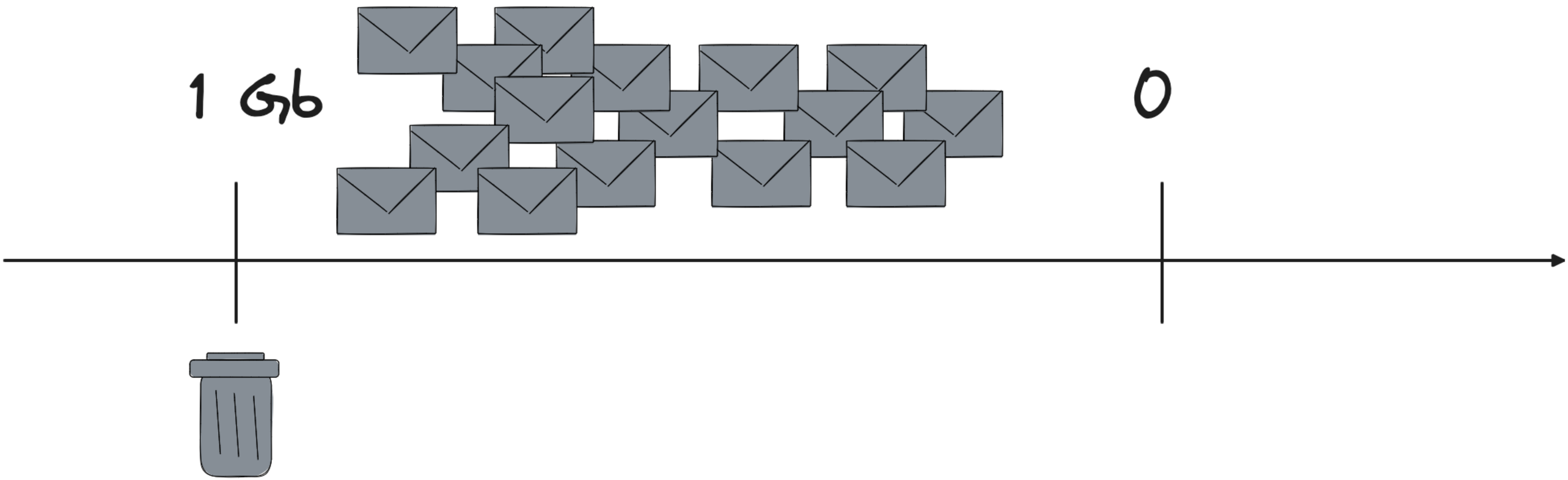
```
{
    "name": "Francesco",
    "amount": "1$"
}
```

```
{
    "name": "Francesco",
    "amount": "7$"
}
```

```
{
    "name": "Francesco",
    "amount": "10$"
}
```

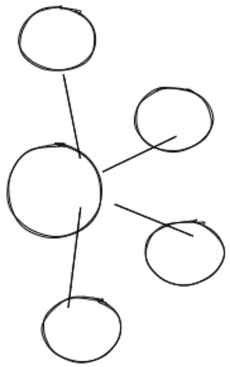
Retention

Retention

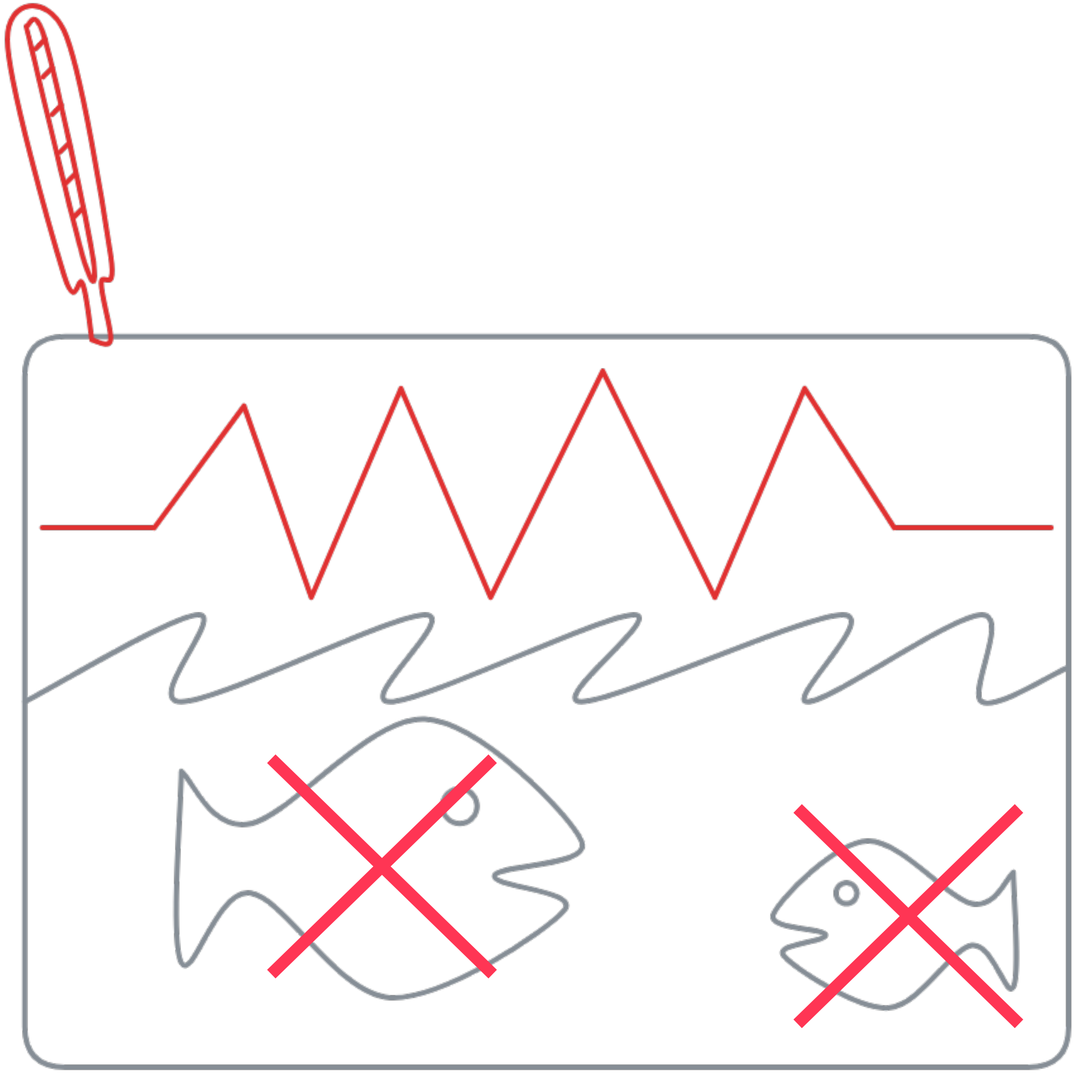


Generating Cascading Effects

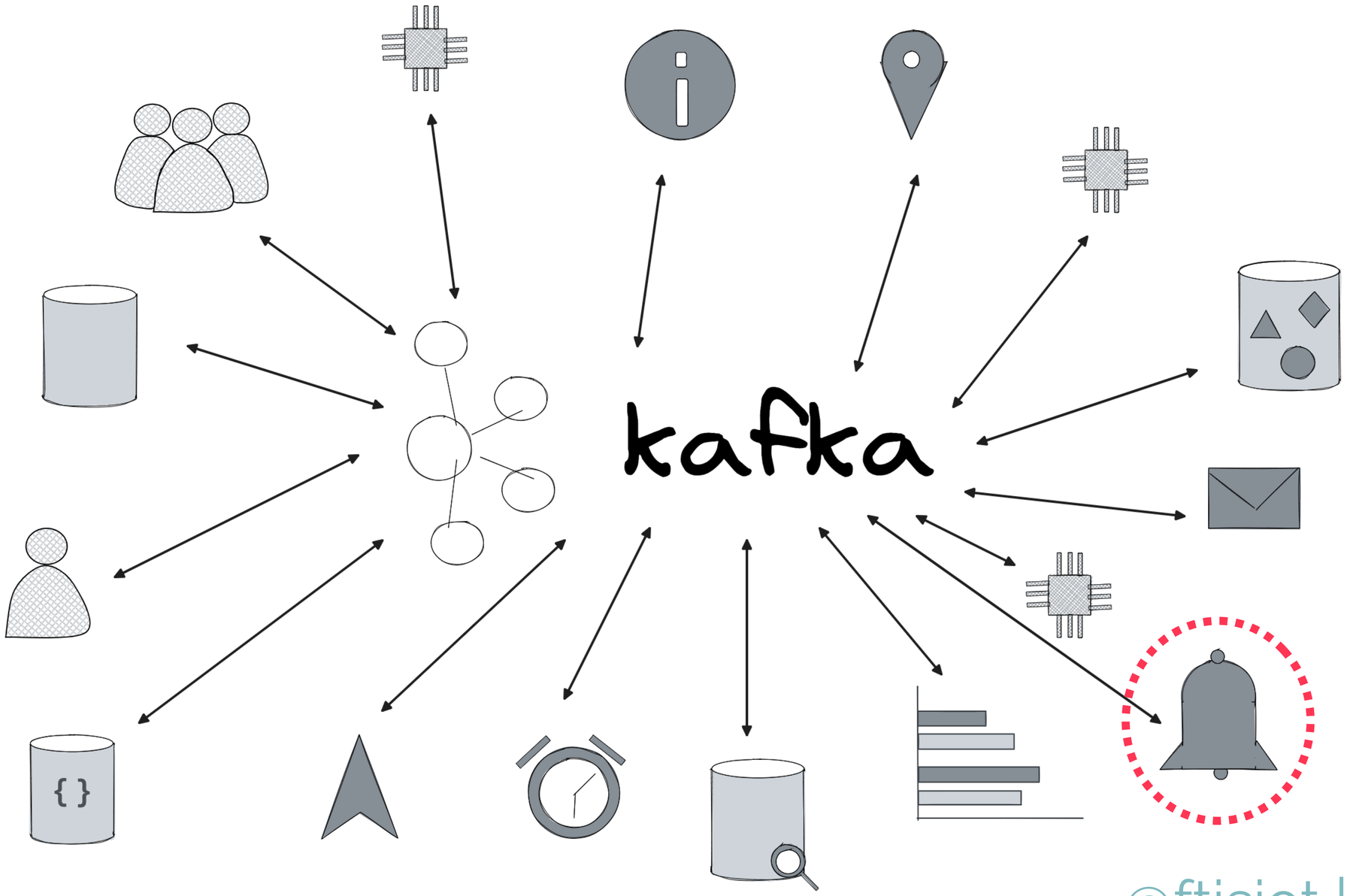
Temperature: 150˚C



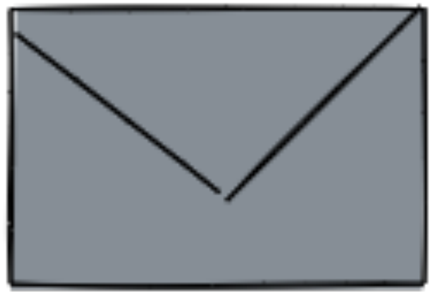
kafka



Gain Access to a Consumer



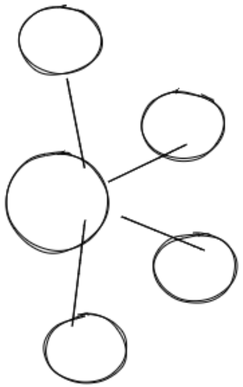
Each message



is only read

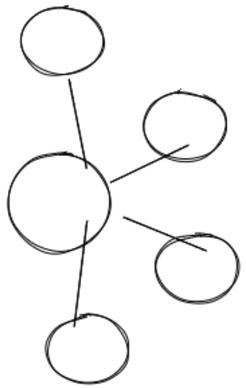
once

per **consumer group**



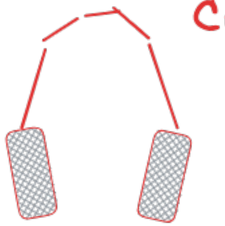
kafka

Consumer: Notification_1
Consumer Group: Notification

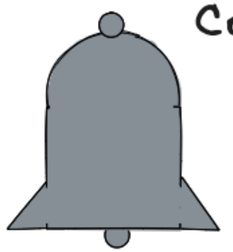


kafka

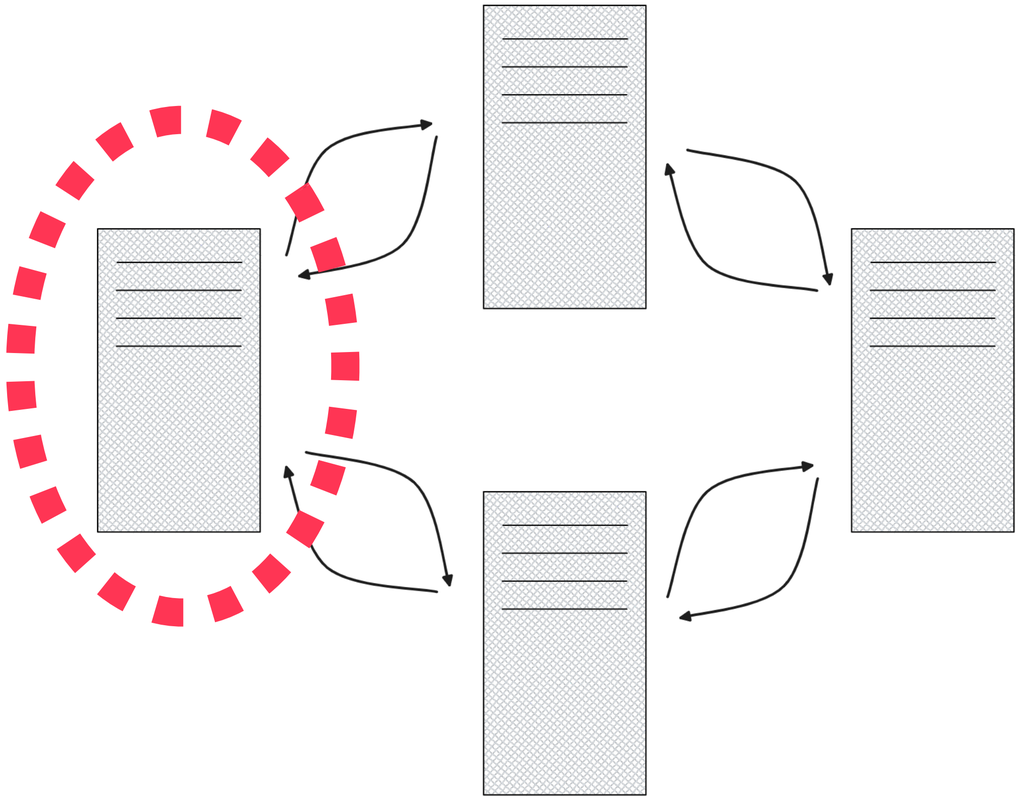
Consumer: Notification_2
Consumer Group: Notification



Consumer: Notification_1
Consumer Group: Notification



Gain Access to a Broker



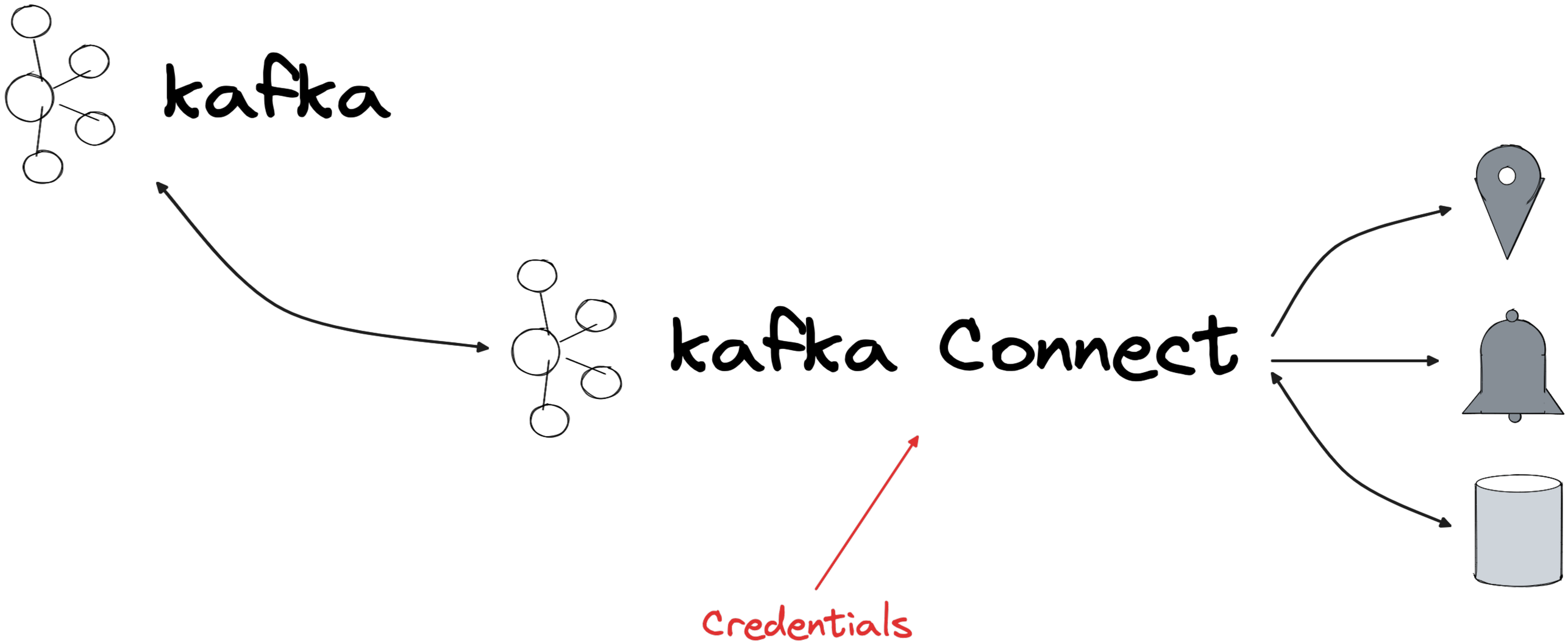
Service Disruption

ALL

in the Data

Credentials

hackers hands


kafka
kafka Connect
Credentials

aiven

How can we be ready?

Francesco Tisiot - Staff Developer Advocate

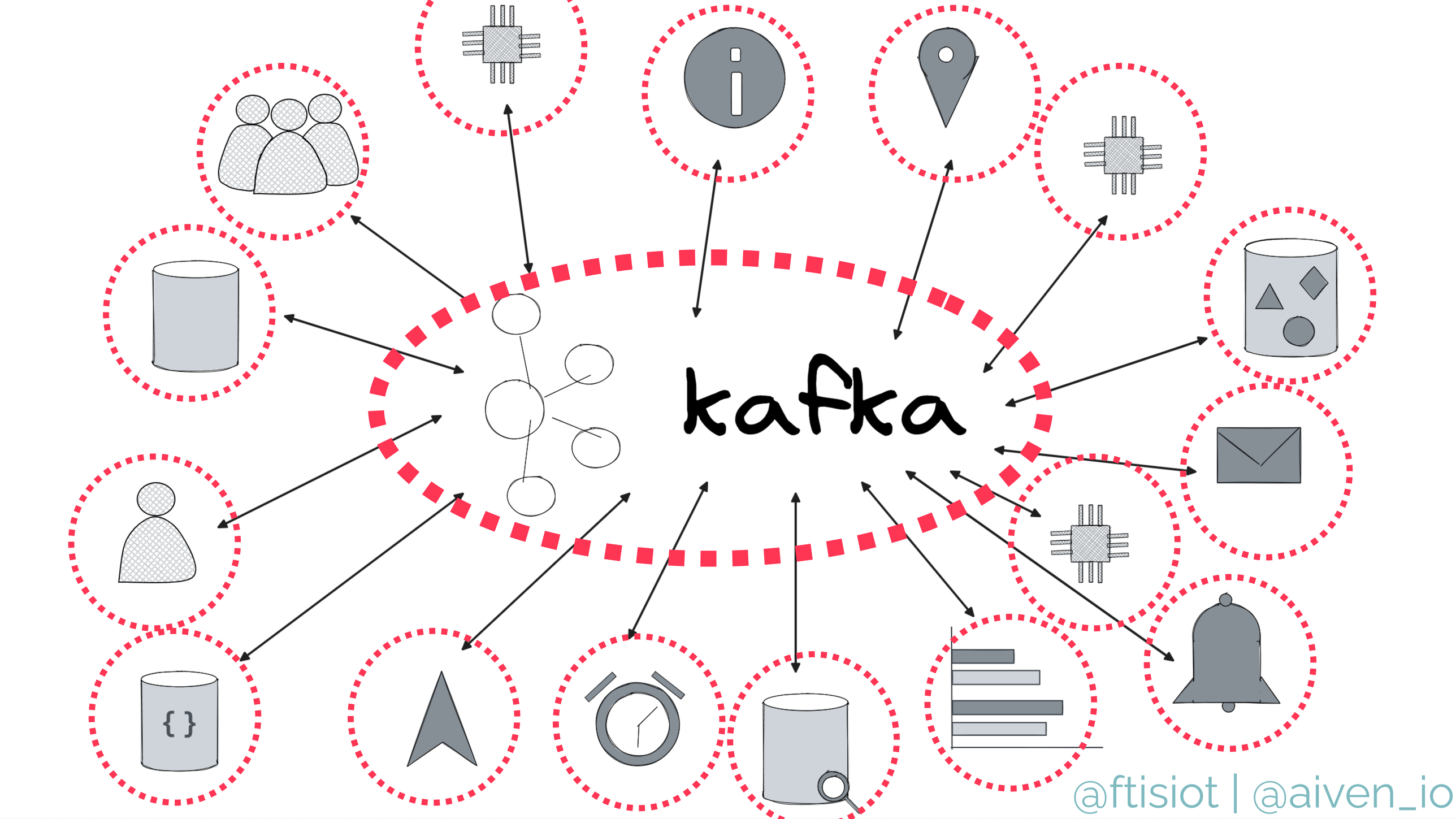
@ftisiot

aiven

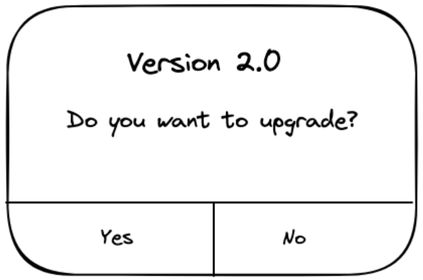
Plan

Francesco Tisiot - Staff Developer Advocate

@ftisiot

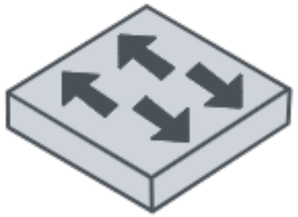

kafka
{ }

Version



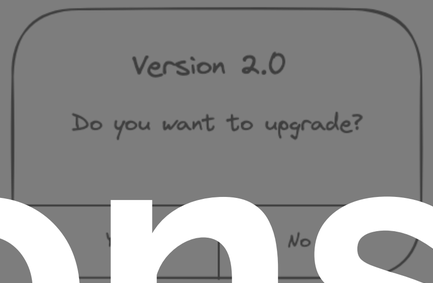
Upgrades

Logging



Communication

Authentication

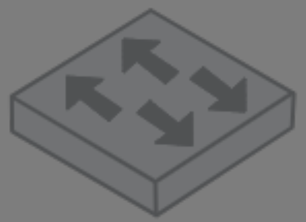


Version

Upgrades

Logging

Responsibility Matrix



Communication

Authentication

Responsibility Matrix

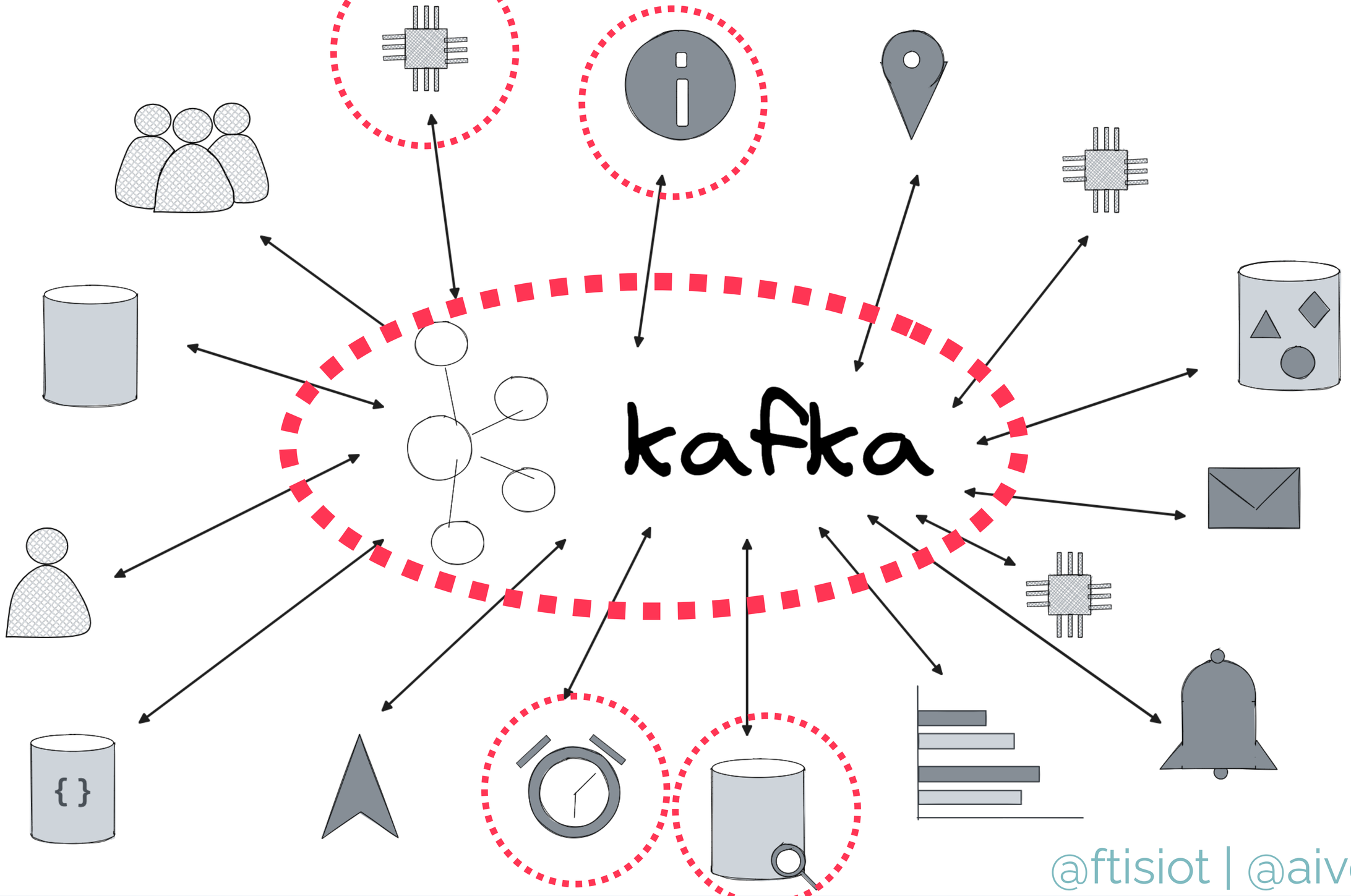
Incident Management

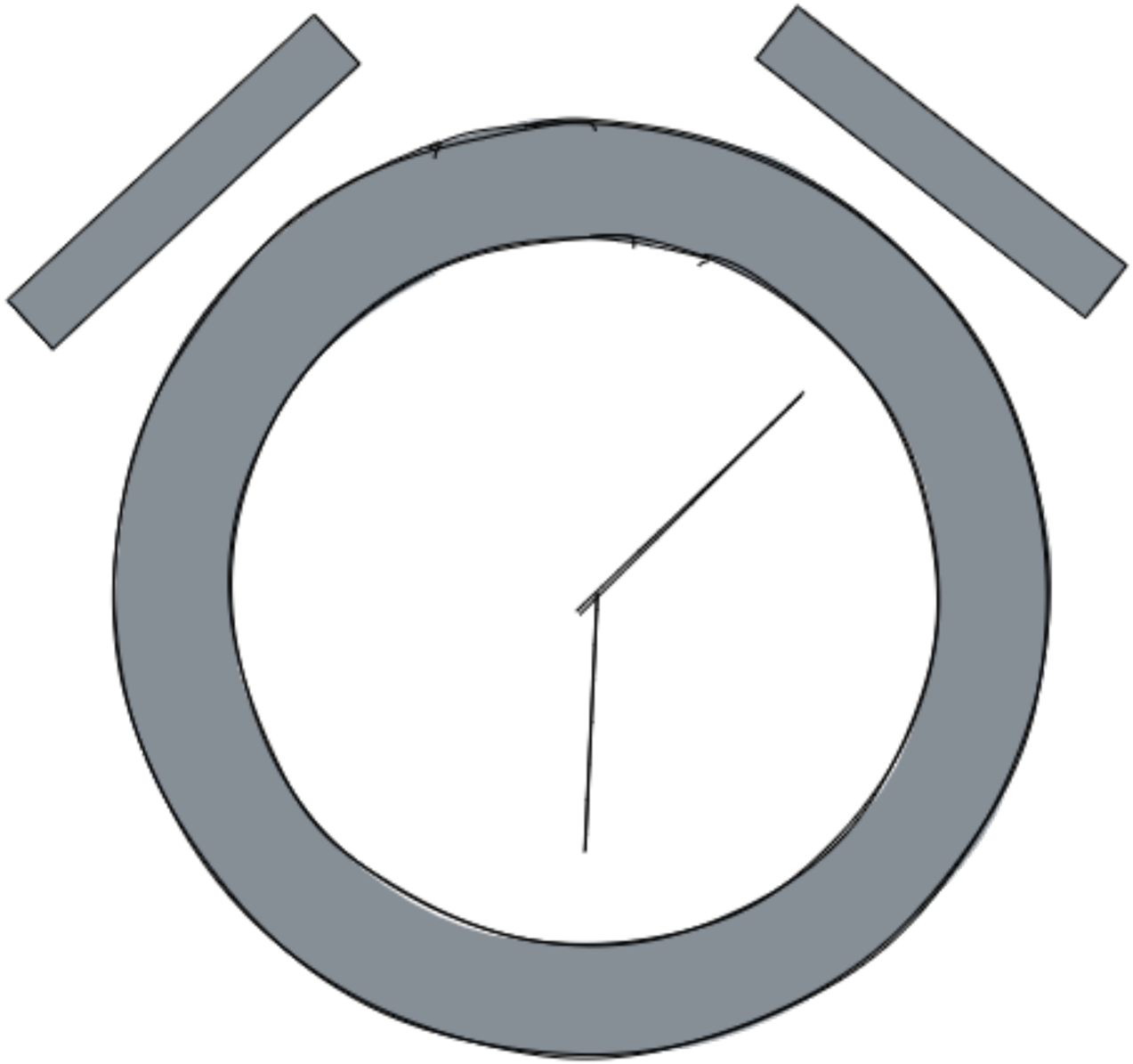
Monitoring

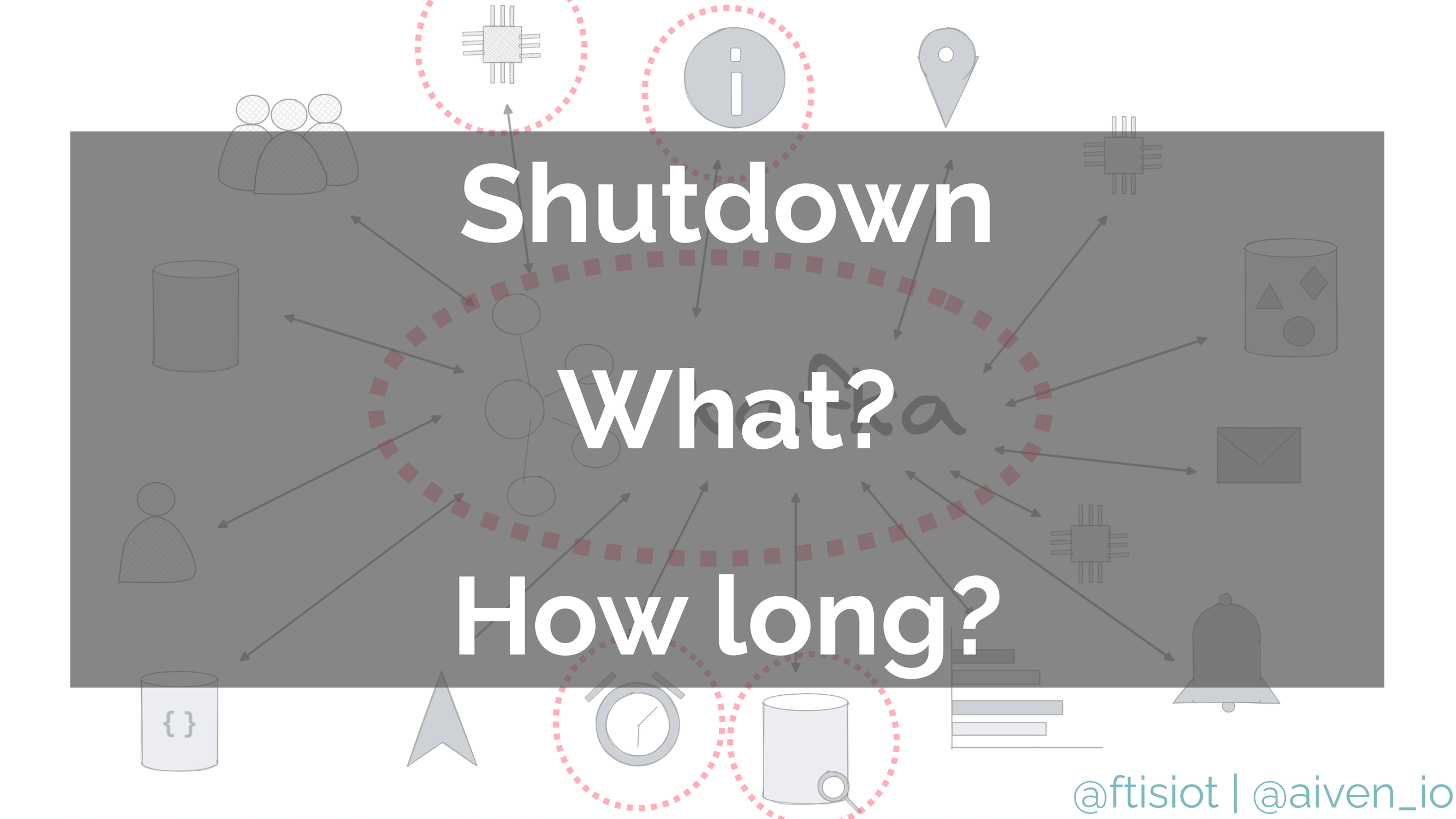
Maintenance
Upgrades

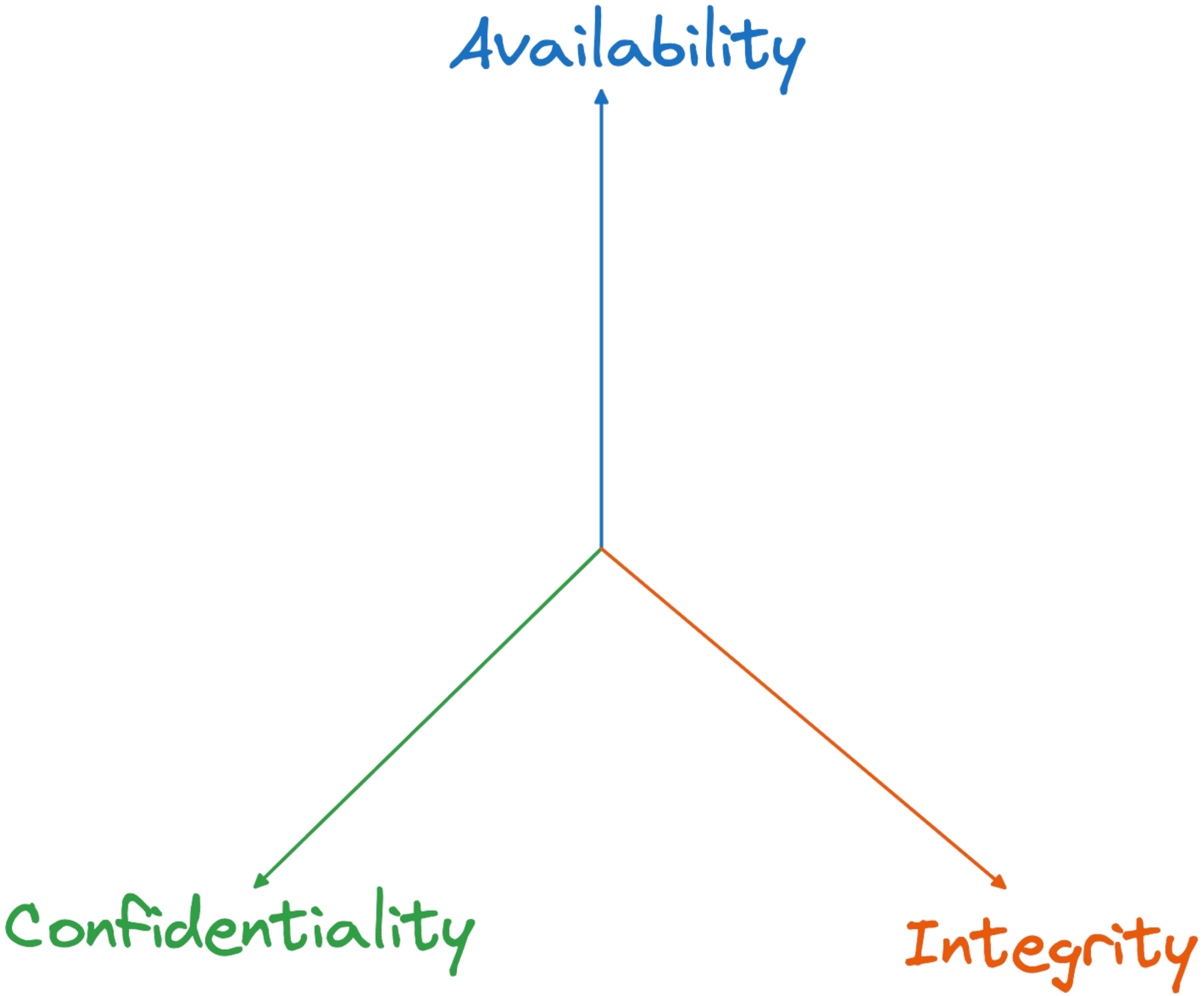
User/Role definition

Access

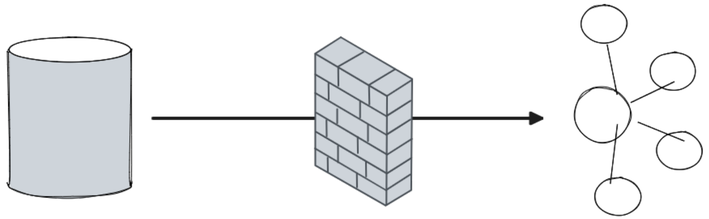

kafka
{ }




Shutdown
What?
How long?


Availability
Confidentiality
Integrity

Contingency Plans



Isolate

Stop Services

Investigate

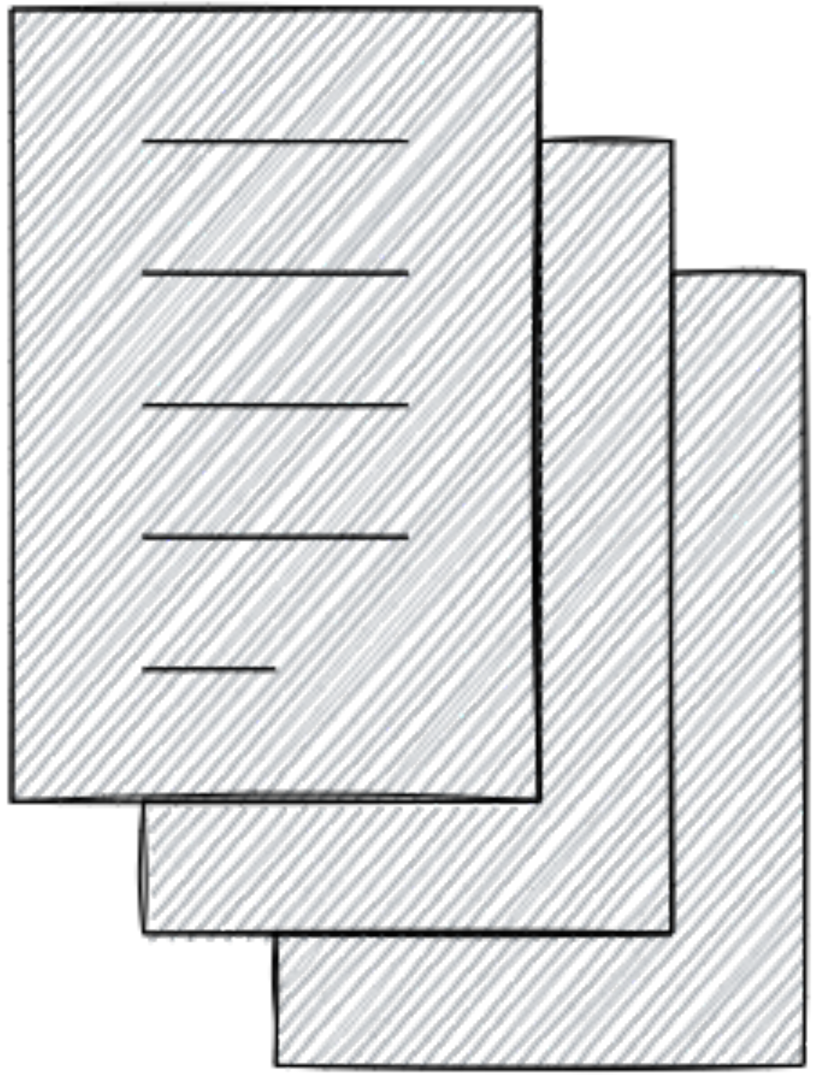
aiven

Execute

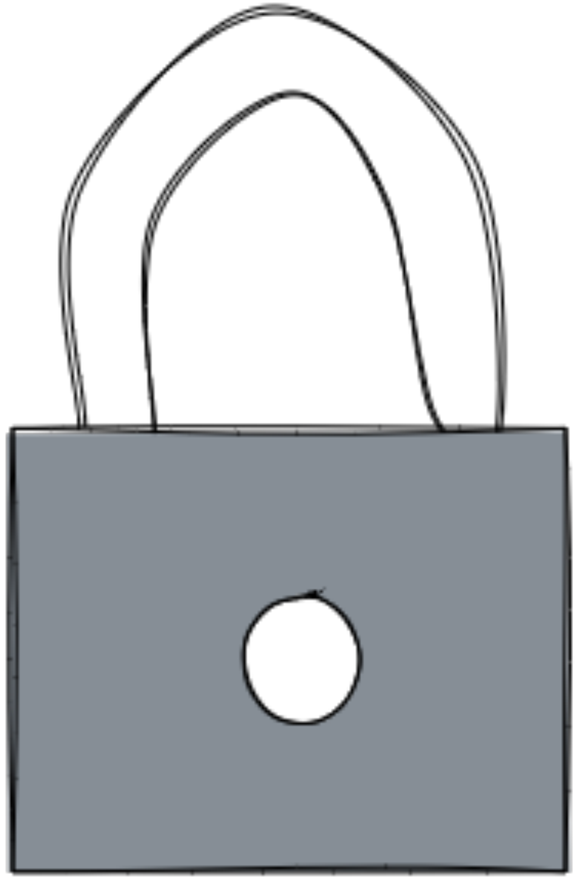
Francesco Tisiot - Staff Developer Advocate

@ftisiot

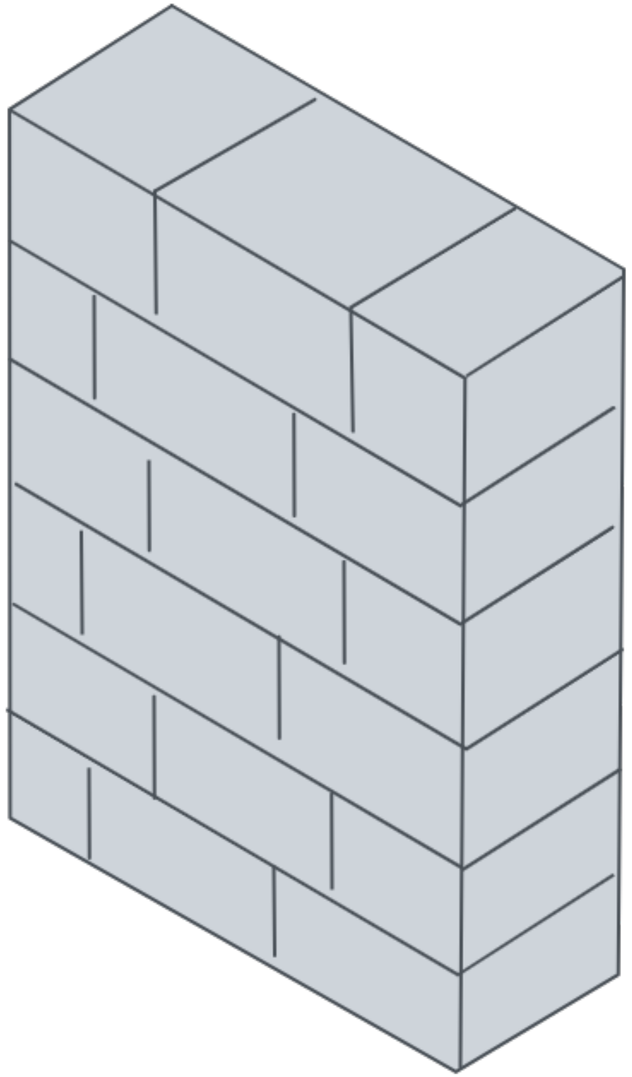
Infrastructure as Code

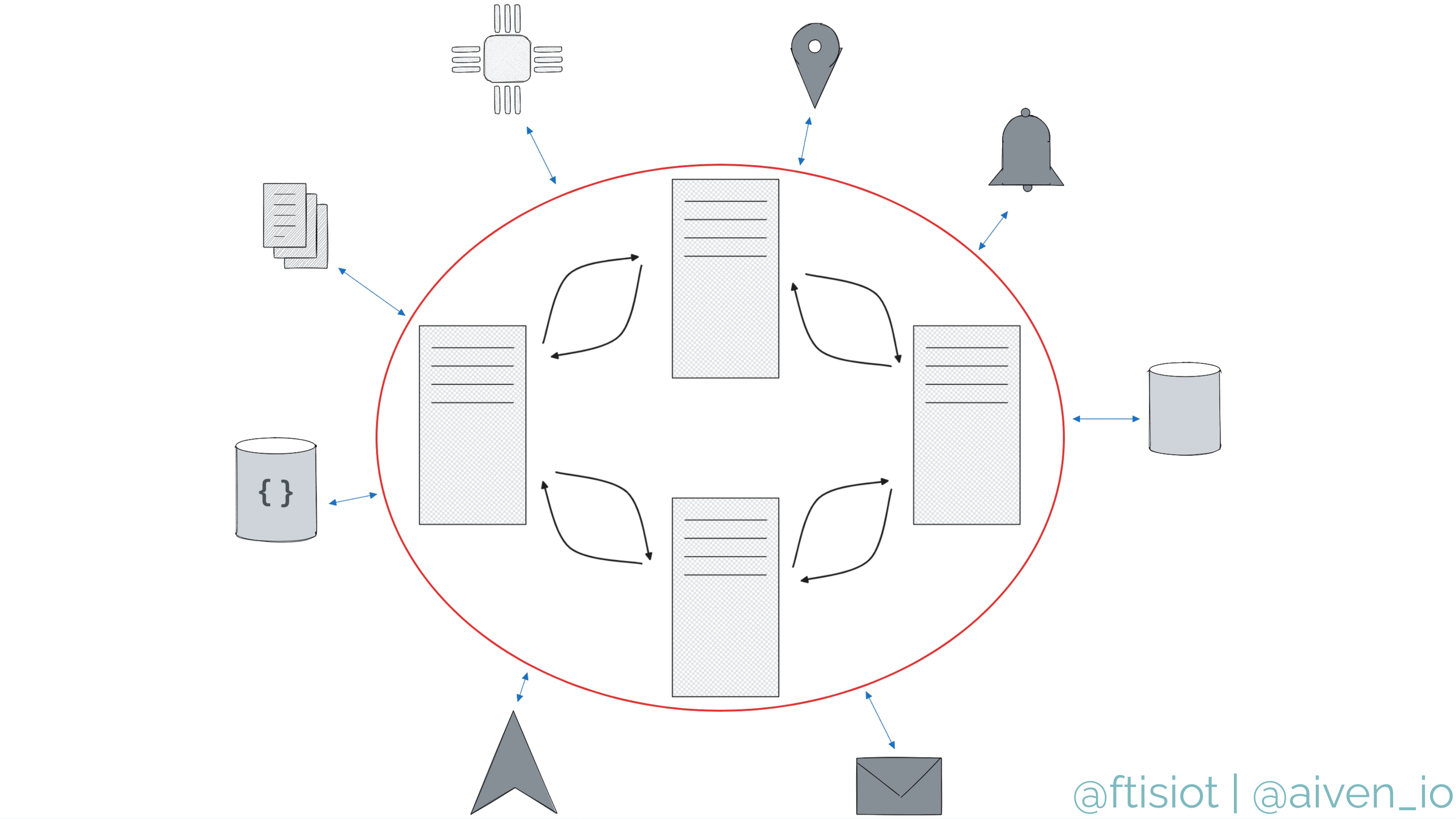


Encrypt



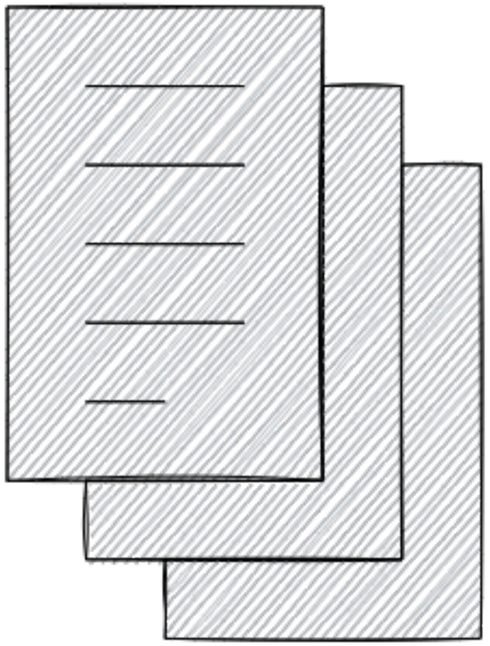
Isolate



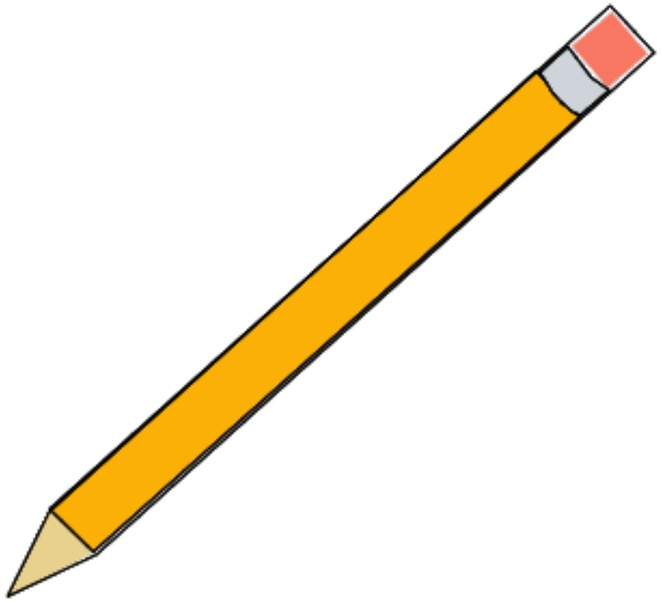


Strict Access Control

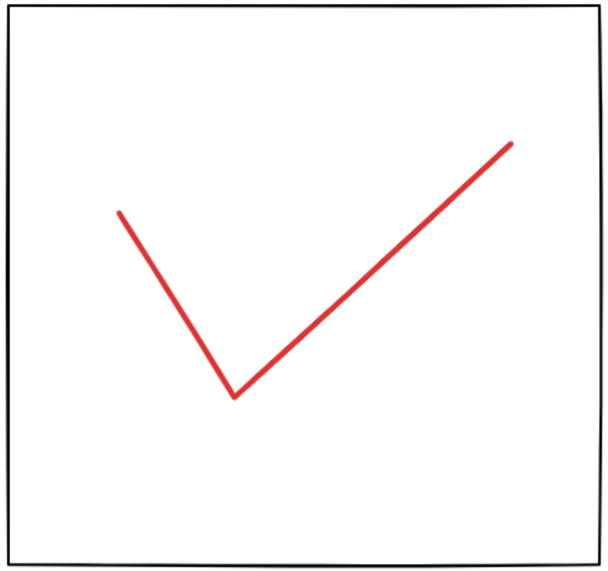
Read



Write



Use Schemas



aiven

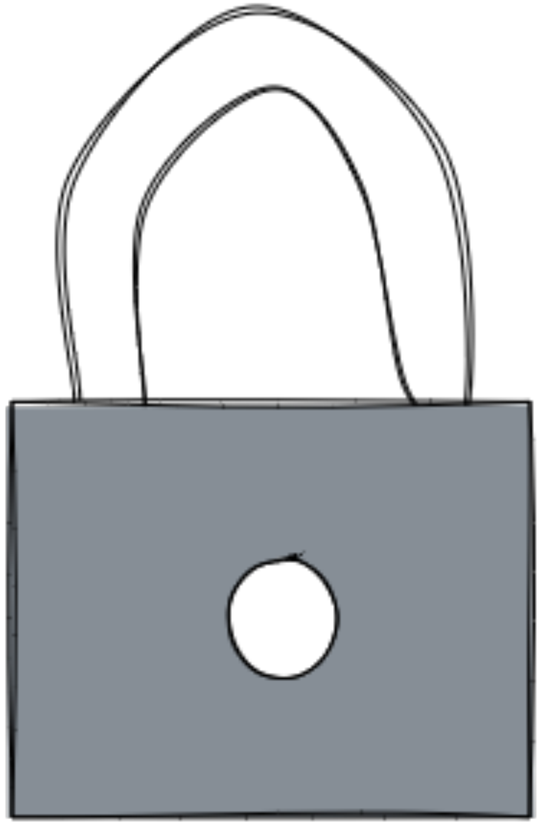
Monitor

Francesco Tisiot - Staff Developer Advocate

@ftisiot

Network

Nodes

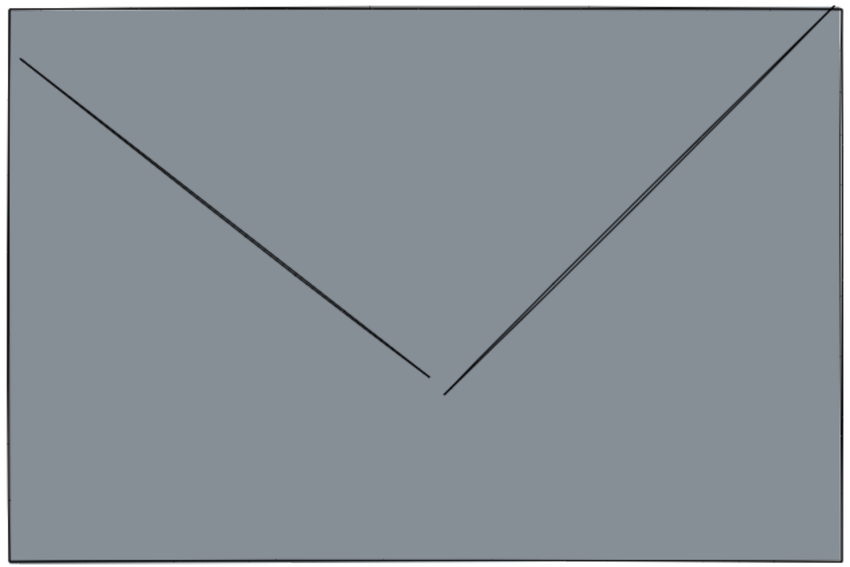


Credentials

IPs

Throughput

Size



Schema

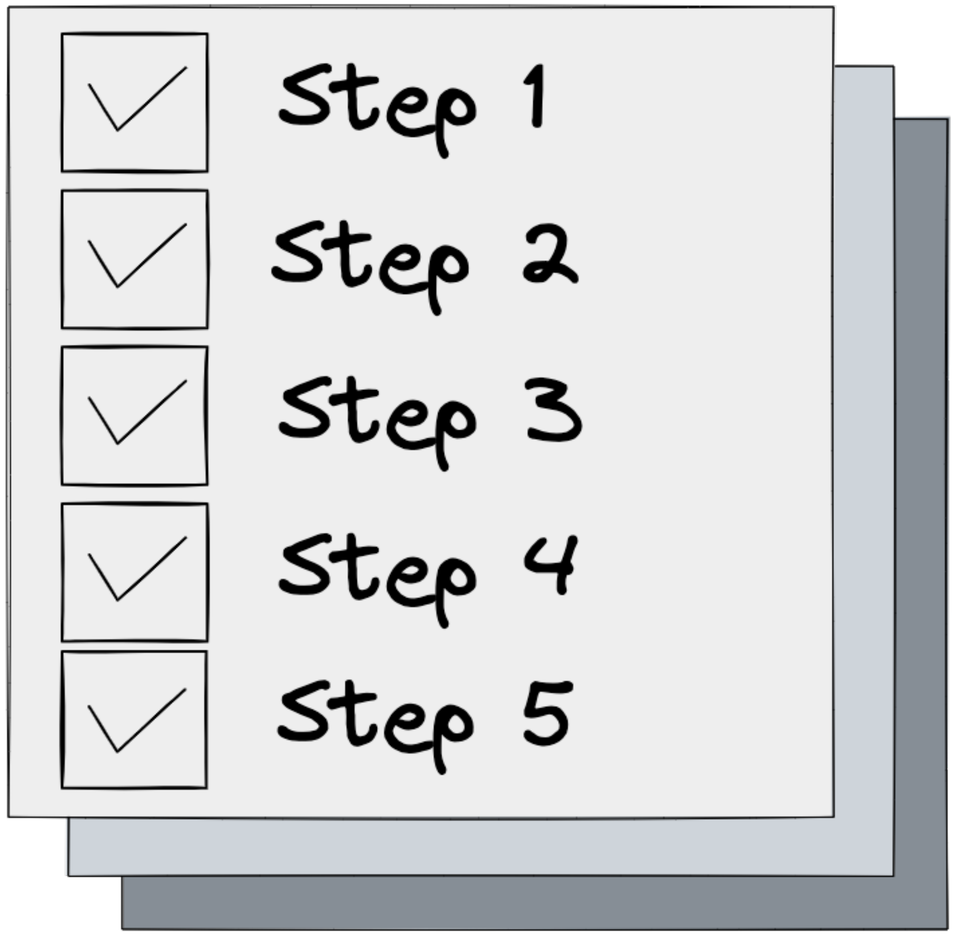
Distribution

aiven

Test

Francesco Tisiot - Staff Developer Advocate

@ftisiot

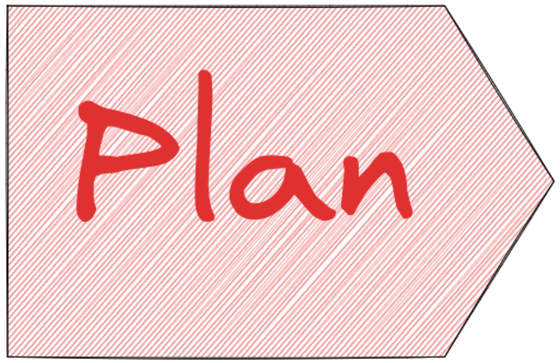

Step 1
Step 2
Step 3
Step 4
Step 5

aiven

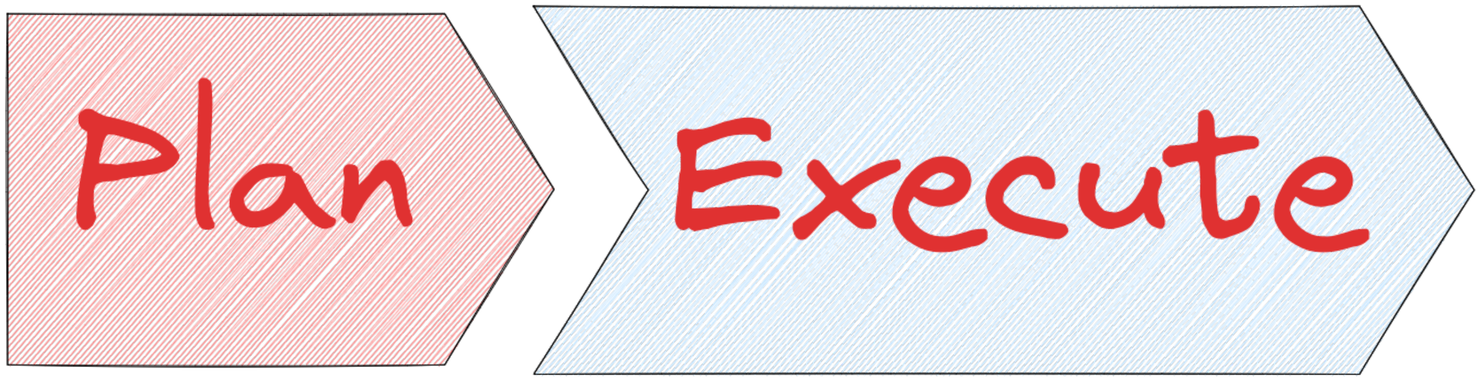
Be Ready

Francesco Tisiot - Staff Developer Advocate

@ftisiot

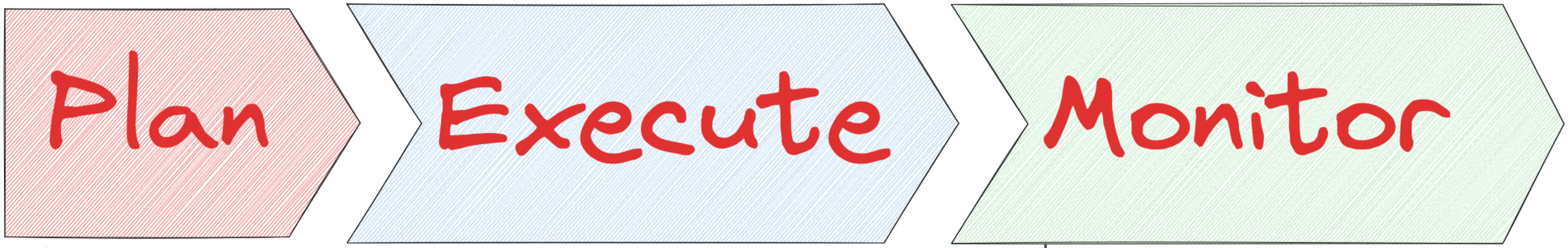


- Estimate attacker's intent
- Map data infrastructure
- Understand criticality
- Define responsibilities
- Define plans



- Estimate attacker's intent
- Map data infrastructure
- Understand criticality
- Define responsibilities
- Define plans

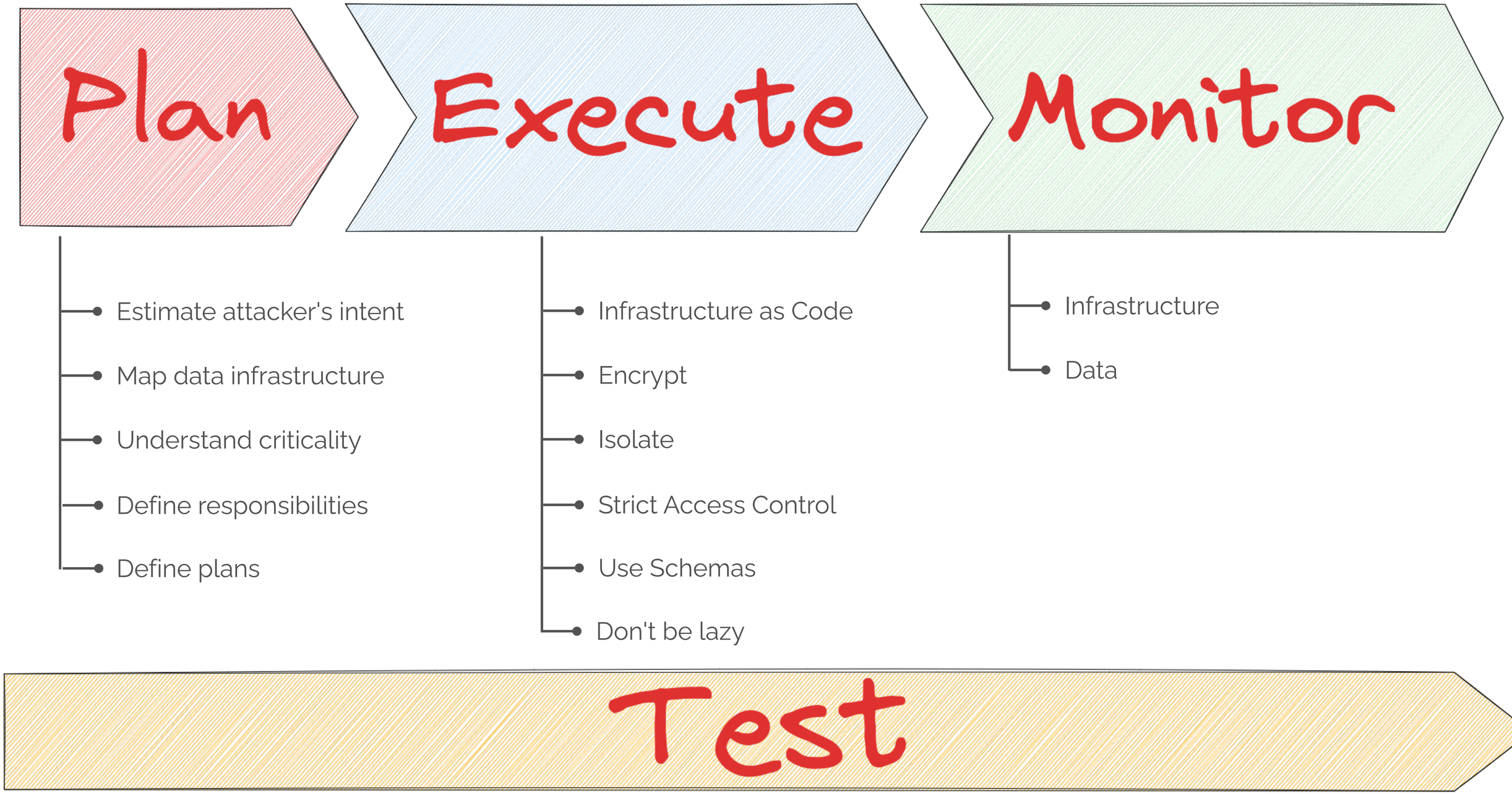
- Code Infrastructure
- Encrypt
- Isolate
- Strict Access Control
- Use Schemas
- Don't be lazy



- Estimate attacker's intent
- Map data infrastructure
- Understand criticality
- Define responsibilities
- Define plans

- Code Infrastructure
- Encrypt
- Isolate
- Strict Access Control
- Use Schemas
- Don't be lazy

- Infrastructure
- Data


Plan
Execute
Monitor
Estimate attacker's intent
Map data infrastructure
Understand criticality
Define responsibilities
Define plans
Infrastructure as Code
Encrypt
Isolate
Strict Access Control
Use Schemas
Don't be lazy
Infrastructure
Data
Test

Encryption

Isolation

Schemas

aiven

IaC

Monitoring

https://go.aiven.io/talk-attack-defend-kafka

aiven

Attacking (and defending) Apache Kafka

Francesco Tisiot - Staff Developer Advocate

@ftisiot