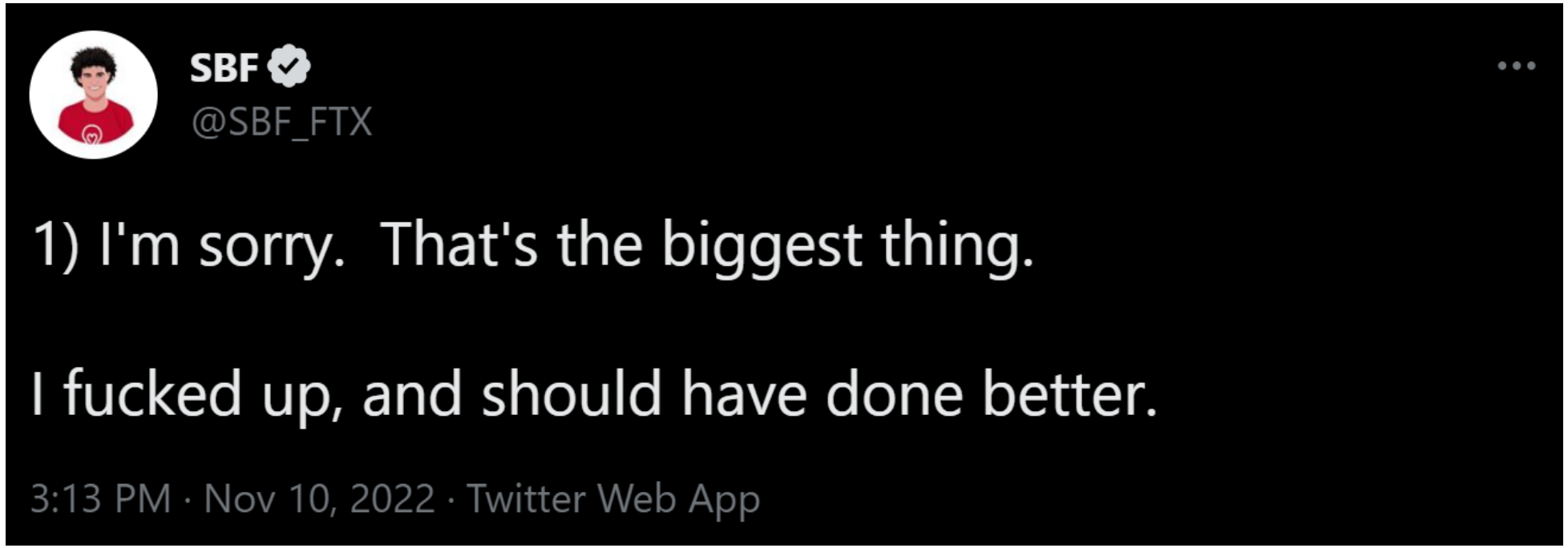
Insights into an alarmingly mission critical application

Christian Tschanz, Swisscom, B2B-PAP-BTU

swisscom

Oh no...

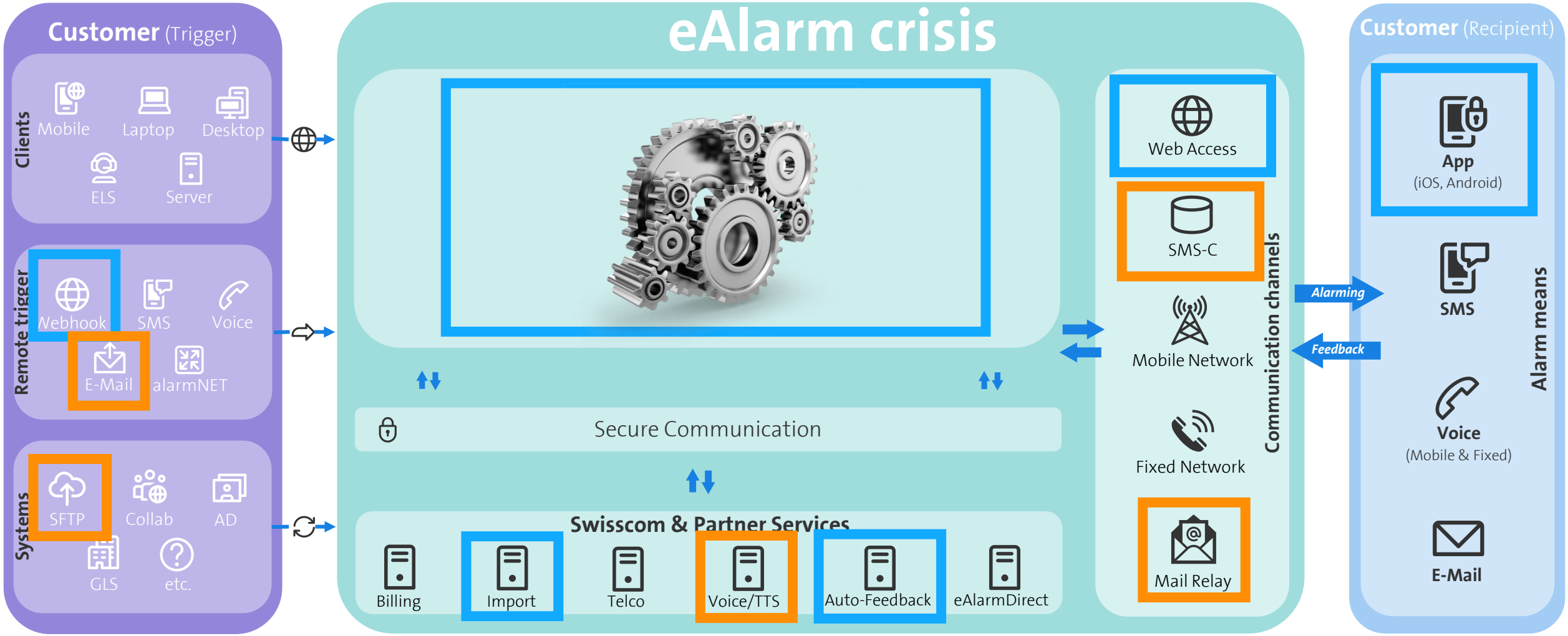
Tell EVERYONE



...start writing emails

« … we alert PEOPLE –
with the right *message*, at the
right *time*, on the right *channels*. »

… from source to *eAlarm crisis* to recipient – and back again.



ALARMING

FEEDBACK / ACKNOWLEDGEMENT

Challenges

Elasticity & Control

- Scaling & Throughput
  - Long periods with no activity… which will change suddenly!
  - Cost saving opportunity but scalability can’t be compromised
- Reliability & Compliance
  - Hot-path of alerting has to be (very) HA
  - PII everywhere!
- Custom & 3rd Party Services
  - Specific needs which can’t be satisfied by every service
  - Custom solutions have the burden of maintenance
- Complexity & Flexibility
  - Faster iteration desired
  - Consolidation of control under our team is desired

Off to the cloud we go...

LANDING ZONE

The iAWS Platform

Interfaces	**Native** | Fleet Management | COTS						
Functional Pillars	Account Vending	Identity and Access Manage-ment (IAM)	Service Mesh & Network	Security & Com-pliance	FinOps	Curated Service Catalog	

Enterprise Landing Zone

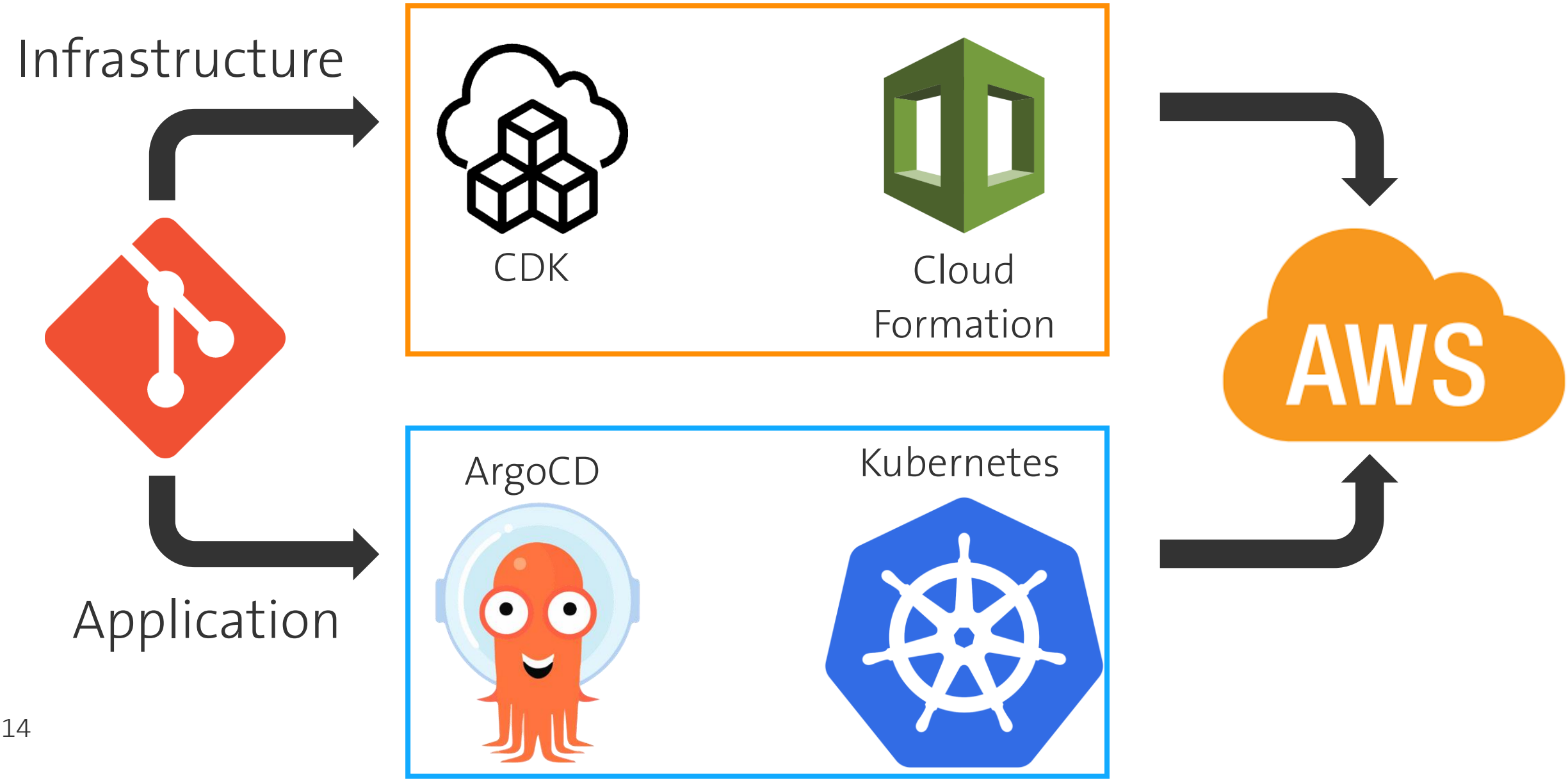
- Centrally Managed
  - Self-service with benefits
  - Your own account but managed but still separate
- Service Catalog
  - Best Practices
  - Designed with Compliance & Security in mind
  - Ready-made Solutions
  - But… you can’t just YOLO it

gg ez 👏

- Reliability & Compliance
  - Compliant by Design
  - Should be reliable, except maybe us-east-1 ;)
- Custom & 3rd Party Services
  - Integrated and capable services ready to use
  - Burden of maintenance shifts to config
- Complexity & Flexibility
  - New patterns are possible
- Scaling & Throughput
  - Lift & Shift will only get you so much

A new workflow

GitOps all the things



But how do I...

Configure the database?

We want:

- Schemas/DBs
- Users
  - Credentials in SecretsManager
- Whatever else your heart desires

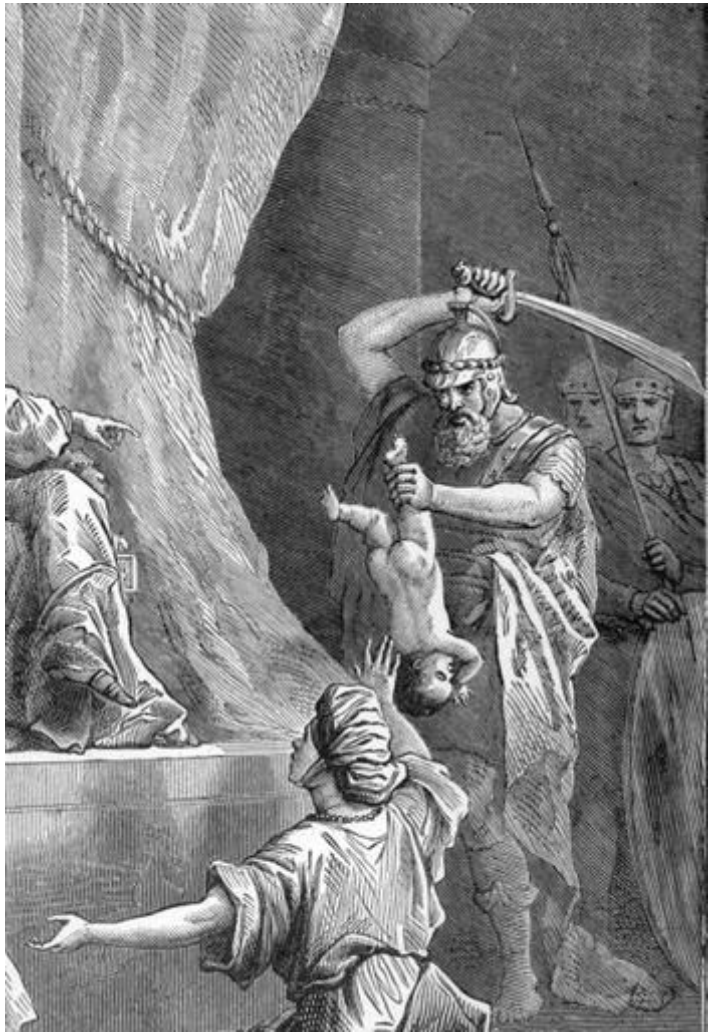
Some things can be setup using parameter & option groups

Hard Manual Labour

Where can we do that?

- Application Track:
  - Operator or similar
  - Apps must handle lifecycle
  - We need admin credentials in k8s
  - You have to go through k8s

- Infrastructure Track:
  - We need to integrate with CDK
  - Part of DB/Infra lifecycle
  - Only expose necessary credentials to k8s
  - You have to go through an Infra deployment



DB Schema Provisioning in CDK – What we want

```python
for schema in props.application_configs.db_schemas:
    db_schemas[schema] = RdsMariaDbSchema(
        scope=self,
        construct_id=f"{schema}-RDSMariaDbSchema",
        props=RdsMariaDbSchemaProps(
            application_name=props.application_name,
            env_name=props.env_name,
            schema_creator_function=db_schema_creator.function,
            secretsmanager_kms_key_arn=cmk_kms_keys["secretsmanager"].key_outputs.key_arn,
            rds_mariadb_admin_credentials_secret_arn=rds_mariadb.mariadb_outputs.credentials_secret,
            schema_name=schema,
        ),
    )
```

- Instantiated just like any other construct
- Lifecycle like any other construct
- Fully declarative

DB Schema Provisioning in CDK – How?

Two things are necessary:

1. A «Custom Resource» to represent the state in your deployment
2. A provider that will execute the desired logic

What this means for us:

1. An instance of the «CustomResource» class of the cdk-lib
   - Define input
   - Link to a provider
2. A Lambda acting as the provider which will execute the necessary commands
   - The CDK provides helpers like the «PythonFunction» class
   - The «official» crhelper Python library will make it trivial to create a well-formed lambda

DB Schema Provisioning in CDK – Custom Resource?

```
schema_crd = CustomResource(
    scope=self,
    id=f"{construct_id}-RDSMariaDBSchemaCRD-{props.schema_name}",
    service_token=props.schema_creator_function.function_arn,
    properties={
        "DBName": props.schema_name,
        "ApplicationName": props.application_name,
        "EnvName": props.env_name,
        "SMKMSKeyARN": props.secretsmanager_kms_key_arn,
        "AdminCredentialsSecretARN": props.rds_mariadb_admin_credentials_secret_arn,
    },
)
```

- This is what's behind the previously shown «RdsMariaDbSchema» construct
- Does some input validation on the schema name as well and prepares the outputs

DB Schema Provisioning in CDK – CRD Provider I

```python
from crhelper import CfnResource
helper = CfnResource(log_level="INFO", boto_level="CRITICAL")

def lambda_handler(event, context):
    """Lambda entry"""
    helper(event, context)
```

- It's just a normal lambda which get's a specific event and expects certain outputs
- crhelper is a very lightweight support lib (~300-400 loc)
  - Helps you structure your lambda correctly and ensures proper responses
  - Convenience functions for long running tasks

DB Schema Provisioning in CDK – CRD Provider II

```python
@helper.create
def create(event, context):
    """Respond to CRD creation"""
    props = event["ResourceProperties"]  # What you passed in with the "properties" on the CRD
    # ... do your things
    helper.Data.update({"CredentialsSecret": db_credentials_secret["ARN"]})  # Update outputs
    return f"RDSDBCreationCRD-{application_name}-{db_name}"  # PhysicalResourceId

@helper.delete
def delete(event, context):
    """Respond to CRD deletion"""

@helper.update
def update(event, context):
    """Respond to CRD change"""
    props = event["ResourceProperties"]  # New "properties"
    old_props = event["OldResourceProperties"]  # Previous "properties"
```

Full Circle

eAlarm Crisis presents a very **spiky** workload pattern with **many 3rd party services**.

- Going cloud-native can lead to direct benefits, both for cost and capability

Swisscom is building an enterprise AWS **Landing Zone**.

- Unburdens the migration project and provides ready-made solutions as well as a solid foundation

New workflow for application Development & Architecture.

- Developer Experience changes, addressing new needs, creating new issues
- Solutions have to take into account new additions to the workflow
- There is no magic ☹