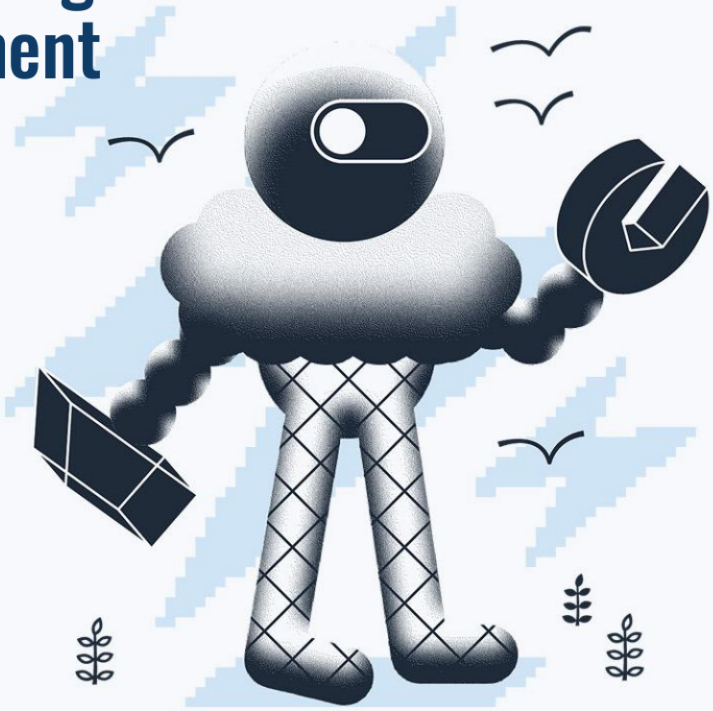
3fs

Lessons learned building secure AWS environment



Jernej Porenta
staff infrastructure engineer

19. October 2023

About

About me

25 years of experience, Linux, DevSecOps, cloud, CI/CD, k8s, …

About 3fs

As engineers and consultants, we develop world-class digital products in **highly regulated industries** and help our customers capture the value of **IoT**.

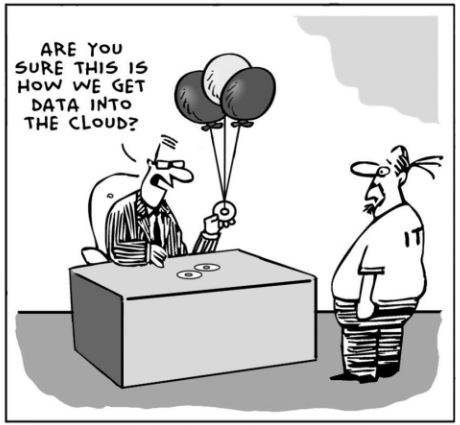
About the project

- digital **assets** custody
- area of involvement:
  - cloud architecture **design**
  - **infrastructure** implementation
  - **devops** ways of working
- code:
  - python, java
  - **microservices**
- timeline: May 2020 - May 2021

About the project

- **compliance** with regulatory requirements in the financial industry (PCI-DSS, DFS Cyber Security Compliant, ...)
- **secure** environment
- built-in **auditing** capabilities
- high **availability** / **scalability**
- **worldwide** presence
- modern **development** flow
- **monitoring** flow

Why AWS



Infrastructure

- Certified SaaS Services
- IaaC
- Fully auditable infrastructure
- High availability
- Scalability

Application

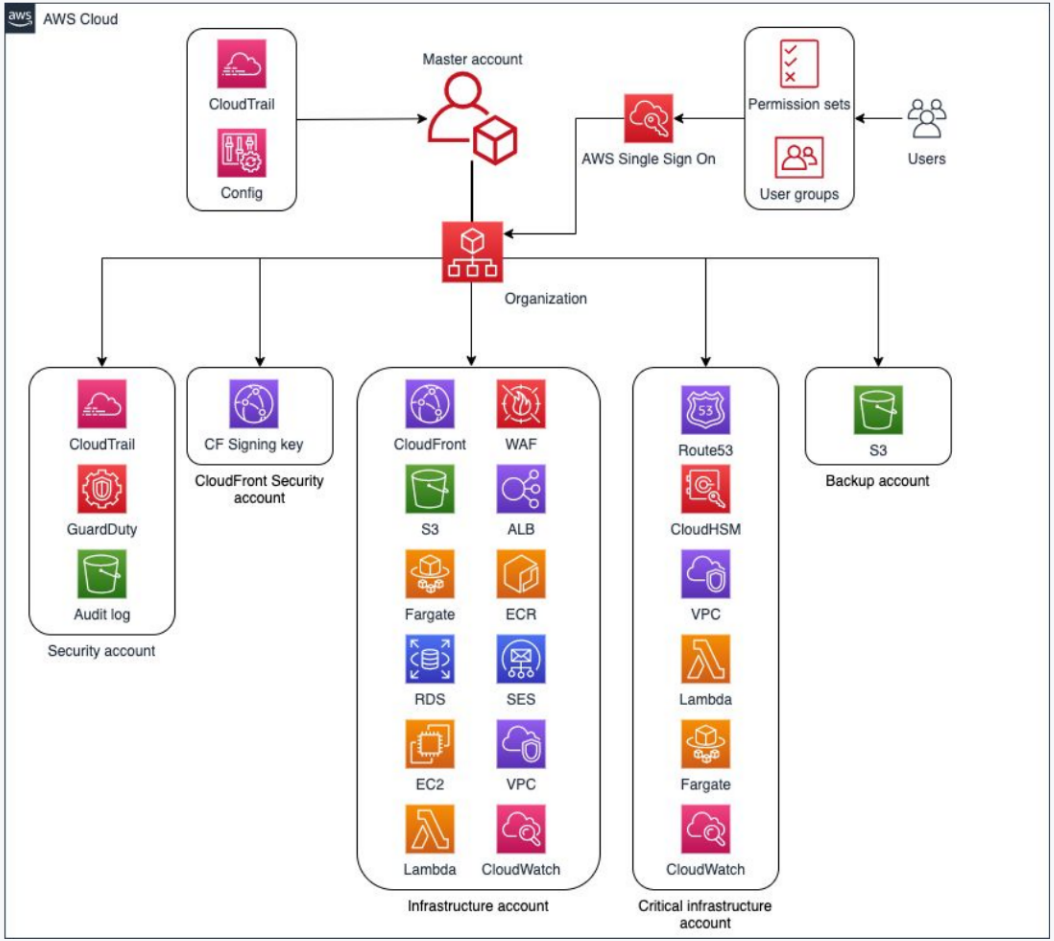
- microservice architecture
- containerised services
- RabbitMQ message broker
- HTTPS API endpoints
- static web page assets
- public key infrastructure

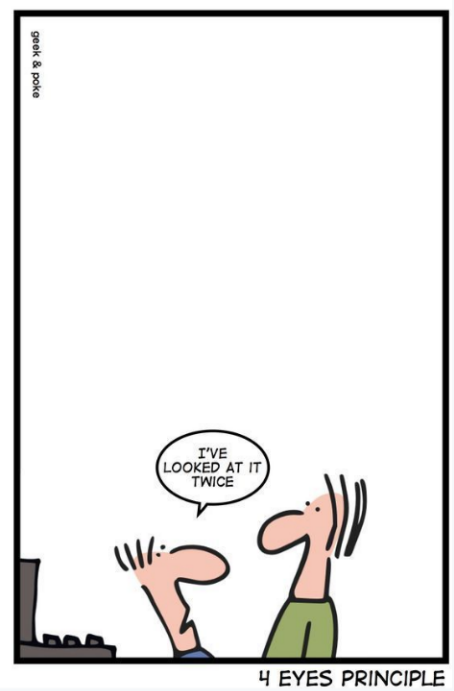
https://maturitymodel.security.aws.dev/en/model/

AWS Security Maturity Model

Accounts organisation

- AWS **Organizations**
- **SCP** - Service Control Policies
- multiple **root** accounts
  - **environments**: dev, staging / qa , prod
  - **internal** infrastructure
- subaccounts
  - **security** account
  - **critical** infra account
  - **infrastructure** account
  - **backup** account





Identity and access management

- AWS **SSO** - Single Sign On (nowadays AWS Identity center) connected to external provider
- **hardware** MFA required - Yubikeys
- **role based** account access
- role **permission sets**
- least **privilege** principle
- non-human accounts: deployments, notification services, …
- **four eyes** principle

IAM Roles and permissions

- organization policy manager
- billing administrator
- cloud trail manager
- developer
- ssm ec2 administrator
- security auditor
- guard duty aggregator viewer
- cloud trail viewer
- sso directory manager
- sso master account manager
- sso accounts manager
- sso settings manager
- system administrator
- deployer
- reader
- guard duty manager
- config aggregator viewer
- …


EC2


Cloudtrail


CloudWatch


Certificate manager


SNS


ALB / WAF


Backup


CloudHSM


CloudFront


SES


S3


SSO


Config


Container Registry


KMS


RDS


Systems Manager


Trusted Advisor


Fargate


GuardDuty


Lambda


VPC

Route53


Security Hub

VPCs

- **Separated** VPCs
  - Infrastructure VPC
  - Blockchain VPC
  - CloudHSM VPC
- VPC **Networking**
  - Network access list, security groups
  - **endpoint** services, VPC peering
  - Application Load Balancers (websockets)
  - Web Application Firewall - **WAF**
  - **CloudFront** CDN
  - VPC Flow Logs
  - custom **DNS** server

Compute services

- **EC2**
  - custom build AMI (packer)
  - Systems Manager Agent
  - no instance metadata endpoints
  - separated subnets
  - RabbitMQ cluster
- **Fargate**
  - read-only containers
  - slim, rootless images
  - separated subnets
- **Lambda**
  - python
  - signed

PKI and CloudHSM

- **Custom CA chain**
  - offline root (shamir secret sharing)
  - intermediates online
  - service intermediates
  - leaf certificates
- **CloudHSM**
  - Thales Luna Hardware Security Module
  - single region service (DR in different region)
  - PKCS#11
  - custom management software (four eyes principle enforced)
  - ephemeral EC2 management instance
- SoftHSM for local development

Security services

- **Systems Manager Parameter store**
  - environment variables store for services
- **KMS**
  - strict key policies
  - local key material
  - IAM managed access to keys
- **security account**
  - collecting all security related information
  - Config, Trusted Advisor, GuardDuty, Security Hub

Credentials management

- shamir secrets algorithm for critical passwords
- manual **onboarding**
  - YubiKeys OTP 2FA
- separated **ownership** of YubiKey and password
- **long lived** credentials for development / staging environment deployment flow
- **short** lived credentials for production environment

Logging and monitoring

- **CloudWatch**
  - custom developer access
  - dashboards
  - alerting
  - SNS topics
- **PagerDuty**
  - alerting based on severity
- **automated** security audits in staging environment
  - ScoutSuite
  - prowler
  - policy_sentry
  - cloudmapper

Development environment

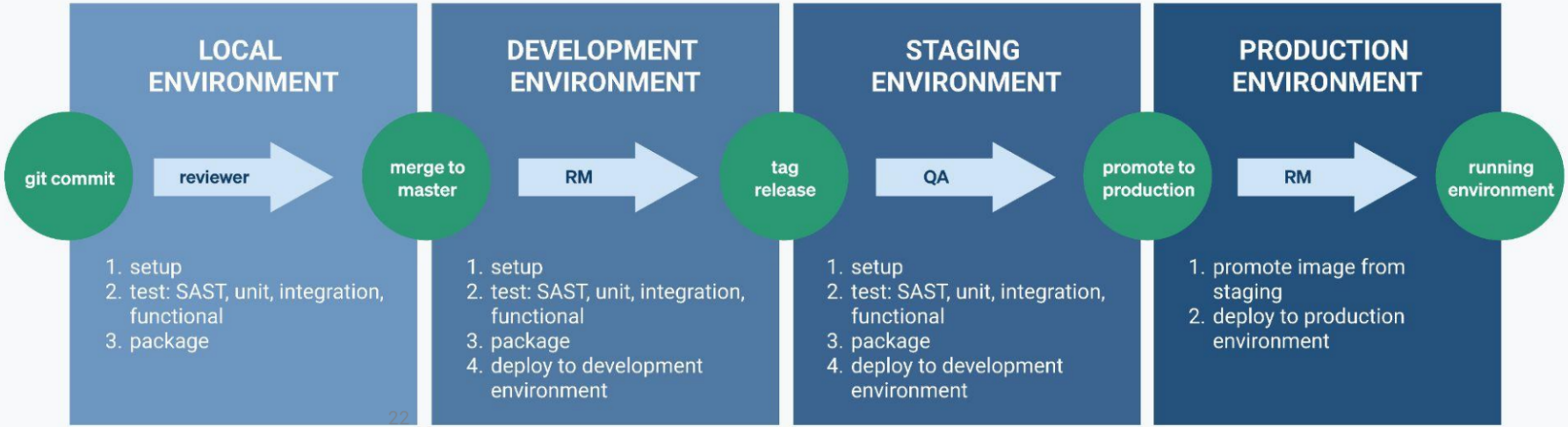
- **AWS hosted** development infrastructure
  - EC2 instances
- VPN and office infrastructure (zero trust approach)
- Yubikey **2FA**
- **Gitlab**
  - streamlined development process
  - GPG signed, peer reviewed commits
  - tight access controls
  - development tracking through Jira
- **Gitlab CI/CD**

Infrastructure development

- Infrastructure as a Code - **IaaC**
  - Ansible
  - AWS CloudFormation
- software deployment **IaaC** container
  - IaaC code
  - IaaC tooling
- development account

Deployments

- **IaaC** with ansible and CloudFormation
- **CI/CD deployments** without user intervention



Lessons learned

Wins

- IAM
- YubiKeys
- CloudHSM
- SCP
- SSO
- streamlined development flow
- naming convention

Opportunities

- long lived credentials
- too early for some services
- long way to develop fully secure AWS environment

Resources

https://github.com/nccgroup/ScoutSuite
Multi-Cloud Security Auditing Tool

https://github.com/prowler-cloud/prowler
Prowler is an Open Source Security tool for AWS, Azure and GCP to perform Cloud Security best practices assessments

https://github.com/duo-labs/cloudmapper
CloudMapper helps you analyze your Amazon Web Services (AWS) environments.

https://github.com/salesforce/policy_sentry
IAM Least Privilege Policy Generator

Resources

https://github.com/99designs/aws-vault
A vault for securely storing and accessing AWS credentials in development environments

https://github.com/iann0036/iamlive
Generate an IAM policy from AWS, Azure, or Google Cloud (GCP) calls using client-side monitoring (CSM) or embedded proxy

https://cloudsecdocs.com/
CloudSecDocs is a website collecting and sharing technical notes and knowledge on cloud-native technologies, ...

https://tldrsec.com/
The best way to keep up with cybersecurity research.

3fs

QUESTIONS?

Blaz Divjak

Dejan Benedik

Marko Dolnicar

Jernej Porenta

JERNEJ@3FS.SI