AWS Organization Security

AWS UG Ljubljana

Anej Skubic

Agenda

1. **Why, how, what?**
2. **AWS Org**
3. **Services** overview & implementation
4. **Wrap up, QA**

Why, how, what?

Cloud observability

AWS SRA

AWS Security Reference Architecture

Tailored to our setup

Tools & services

Terraform, bare-bone, *legacy*

CloudFormation StackSets

AWS Config

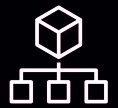
AWS GuardDuty

AWS Inspector

AWS Detective

AWS Security Hub

AWS Org structure



Root account

Try not to use it
Delegate everything

Security OU

Logging account
Tooling account

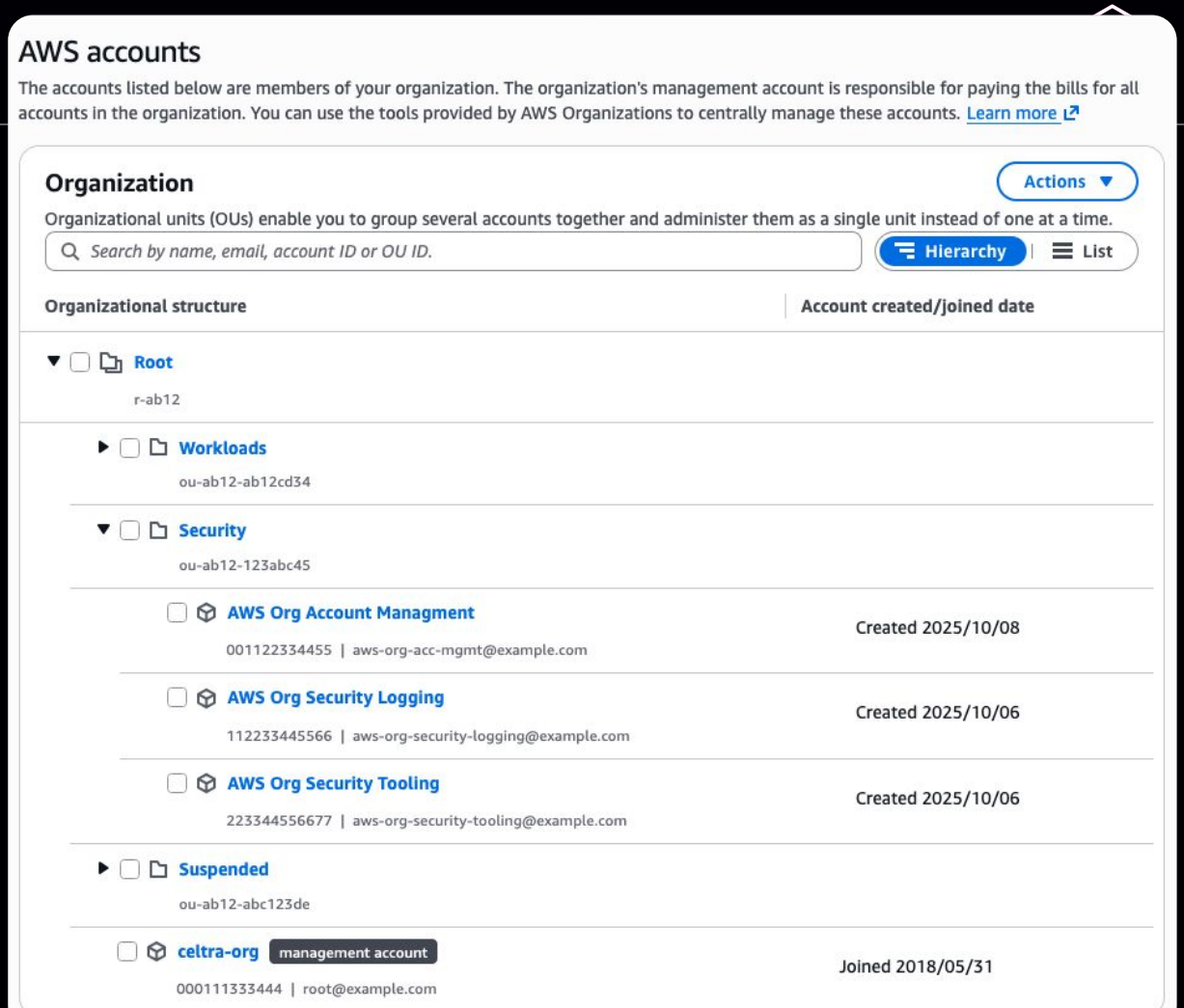
Workloads OU

Development
Testing
Production

AWS Org structure

Root account

Try not to use it
Delegate everything



AWS Config

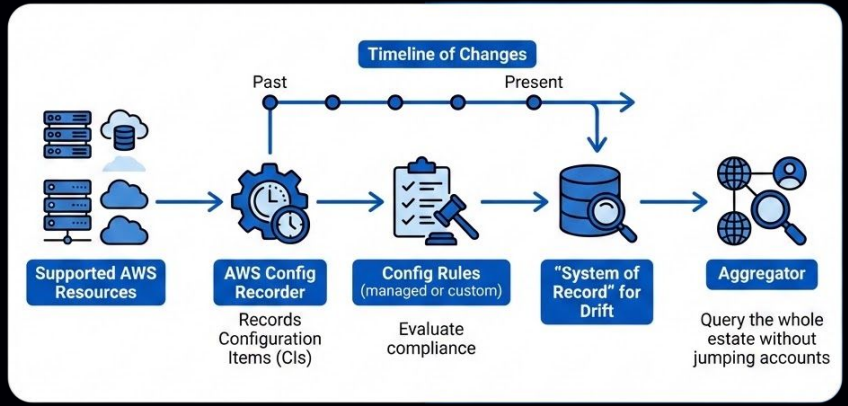
Purpose: configuration history & compliance evaluations for AWS resources

Gives:

- what changed, when, whom*
- rule-based compliance

Concept:

- Config recorder, CI
- Delivery channel
- Config Rules
- Conformance packs



*GenAI infographic

AWS Config

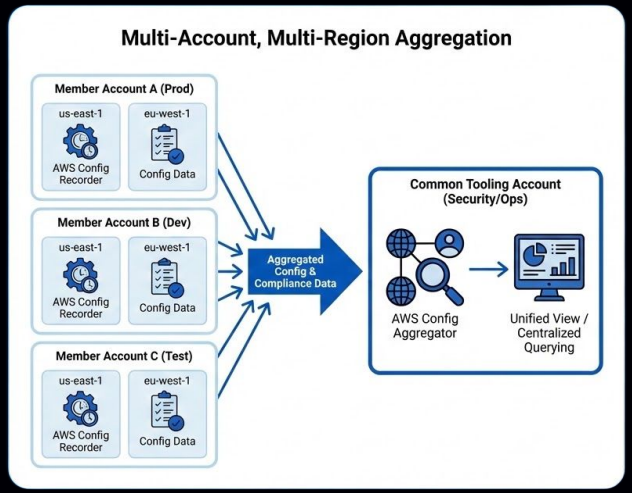
Purpose: configuration history & compliance evaluations for AWS resources

Gives:

- what changed, when, whom*
- rule-based compliance

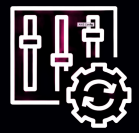
Concept:

- Config recorder, CI
- Delivery channel
- Config Rules
- Conformance packs



*GenAI infographic

AWS Config



- CloudFormation StackSets
  - Per account & region
  - SL Role*, Recorder*, Delivery Channel
- Aggregator in Tooling account
- Root account Recorder

AWS GuardDuty

Purpose: managed threat detection using AWS telemetry

Gives:

- security findings with severity, affected resources, and recommended actions

Concept:

- Detector, Findings
- Data sources and Features (runtime monitoring)
- Malware protection for S3

AWS GuardDuty

- Detector in Tooling account
- Delegated admin
- Org configuration
- Root account

AWS Inspector

Purpose: automated vulnerability discovery and continuous scanning for supported resources

Gives:

- vulnerability findings (CVEs, package exposure), often with exploitability context and fix guidance

Concept:

- Scan types, Findings

AWS Inspector

- Deploy scanner
- Delegate admin
- Org configuration

AWS Detective

Purpose: investigation service that builds relationships/timelines from AWS activity data to explain incidents faster

Gives:

- investigative views (entities, timelines, relationships)

Concepts:

- Behavior graph
- Entity

AWS Detective

- Create a Graph in Tooling account
- Delegate admin
- Org configuration

AWS Security Hub

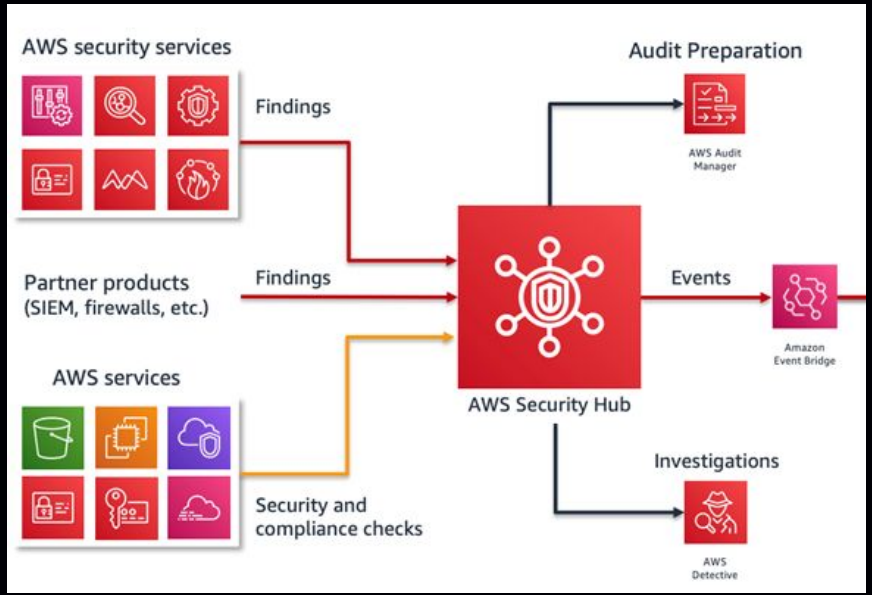
Purpose: centralized security findings and posture management across accounts/regions

Gives:

- Normalizes findings and aggregates from AWS services & partners
- Single pane of glass

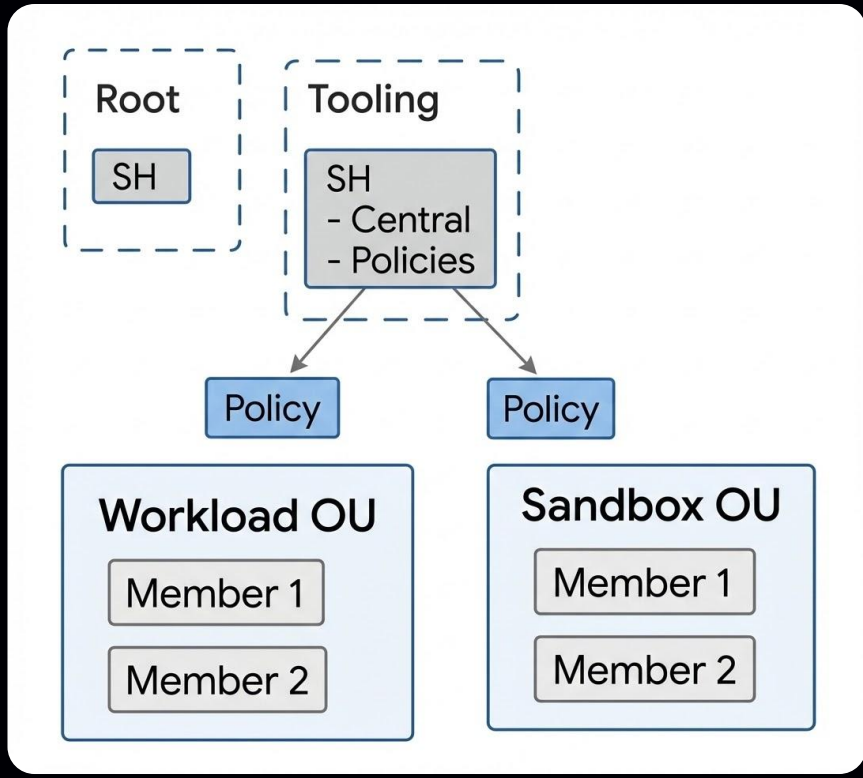
Concept:

- Security standards (Controls)
- Findings
- Insights



AWS Security Hub

- Enable in Tooling account
- Create aggregator
- Delegate admin
- Org configuration
- Policy for enabled standards
- Enable for root account



Wrap Up

- Enable other services
- Disable Root users
- Get over your backlog
- Check what fits your needs (LZA, CfCT, ATF)

QA

Celtra

Thank you!