The Commission's path to Cloud Security Excellence

Belgian Cybersecurity Coalition, 20/06/2024

Nicolas Kyriazopoulos-Panagiotopoulos
DIGIT.C.1.001 – Cloud Centre of Excellence

Who we are

European Commission

+ 70 European Institutions, Agencies or Bodies

Common Cloud Procurement

Separate Governance, IT Strategy and Security Policy

DIGIT.C.1 is here but contributes to both

I am here with the role of the **Commission** Landing Zone Program Manager

European Commission Cloud Strategy

Published in 2019

“cloud-first approach with a secure hybrid multi-cloud service offering”

Cloud-first: initially for new systems, now first steps into migrating legacy

Hybrid: the data-centre is modernised according to cloud principles too

Multi-cloud: too big of a customer to lock in to one provider

Secure: today’s topic

Challenge 1: hybrid

Commission is a political organisation, hosting also systems where the Member States are data controllers.
➔ In these cases, they can object to using a Cloud Provider as sub-processor.

We need a working, secure data centre, even if we accept it won't compete in functionality with the hyper-scalers.

➔ Our resources are split

➔ Pioneers went to public cloud before the central services were ready

Challenge 2: multi-cloud

- High use of both AWS and Azure
- Lower use of OVH Cloud, IBM Cloud

➔ At the minimum: need for 2 landing zones

Challenge 3: secure in a political org.

- No central CTO / CIO imposing technological choices
- Instead: HR Directorate for Security imposing high level contractual rules for *outsourcing (ex: public cloud)*
- Directorate General for Digital Services imposing specific technical standards (in practice enforceable mostly on the DCs managed by DIGIT)

➔ Two different approaches and sets of rules

- Directorate Generals (~ Ministries) can opt out of compliance rules by accepting the risk and informing the governance

Situation in early 2023

- Not a PoC anymore
- Over 200 teams, half of them operating their environments in a decentralised way
- Some observability enforced centrally (security log collection etc)

- No major data protection incidents, cloud accounts are by default isolated

- But... first warnings.

Even a development account can be compromised to spawn 100K worth of bitcoin mining machines in minutes

Learning #1

- Your existing teams will not be familiar with all cloud services, pioneers are needed to bring knowledge to the organisation

#1 **DO FORCE security observability and financial responsibility to those pioneers**

Towards a mature Landing Zone

European Commission

Recapping the requirements

- Landing Zones for AWS and Azure
- To be installed on 600 pre-existing accounts
  - At reasonable cost and within 2 years
- Switch from “high level” contractual requirements to specific guidance
- Scale
- Allow system owners to declare exceptions

Solution: Tooling-informed policy

- We knew we could deploy Cloud Security Posture Management (CSPM) and Cloud Native Application Protection Platforms (CNAPP) easily

- What if we defined the security rules so that they're *easy to implement* by these tools?

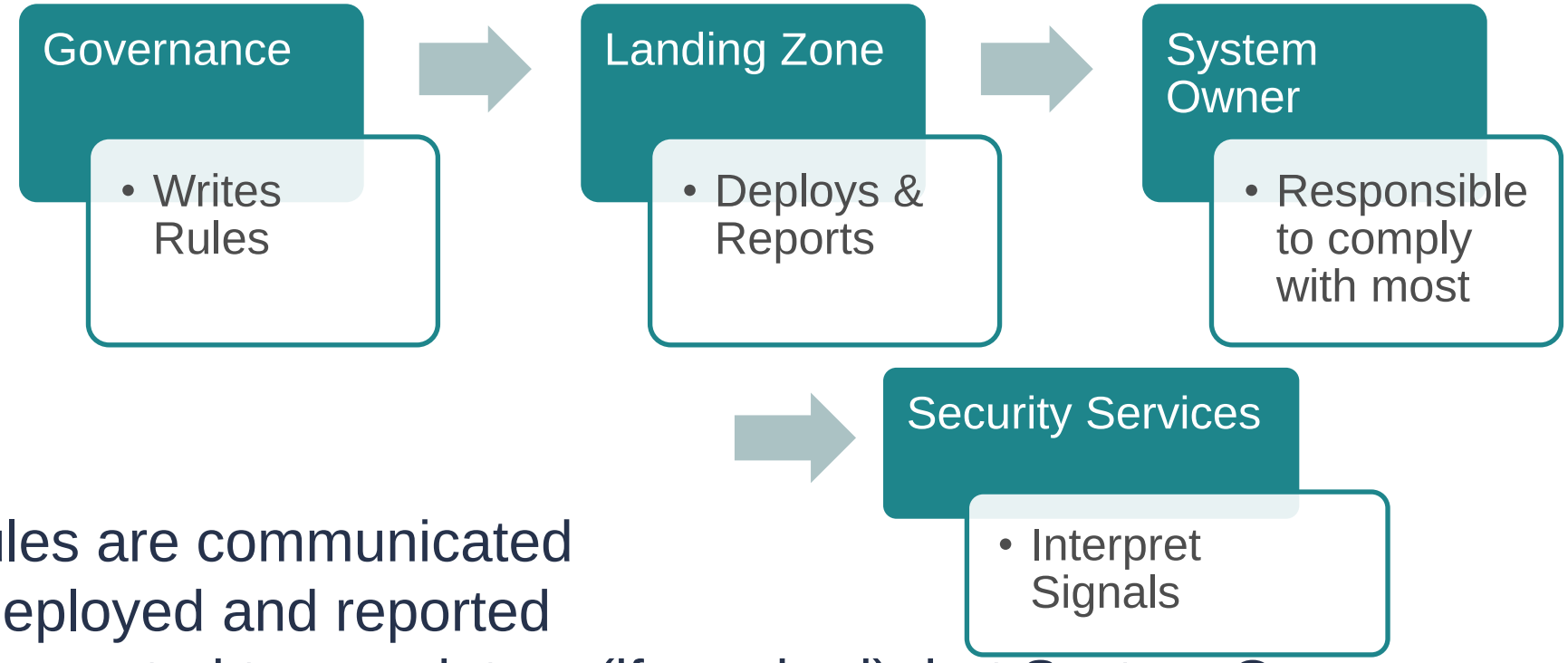
➔ Joint effort between business, IT and Security teams

➔ Started from industry benchmarks (CIS, Azure, AWS)

➔ Complemented with rules inspired from our data centre standards

➔ Permanent committee updating and communicating the rules

The Roles



New rules are communicated
Then deployed and reported
Then converted to mandatory (if required), but System Owners can self-declare exceptions ➔ **Exceptions as a change management tool**

“You’re secure because I attest you did your architecture correctly”

The Tools

- **Azure Policy** provides *exactly* what we want: compliance tools that work regardless of how you deploy, even for ClickOps. Only 1st party tools can do that. Mature exception management.
- **AWS** compliance tooling (mostly 3rd party) works at IaC level. Harder change management: forces the use of 2-3 specific IaC languages.

- **In Commission**: additional requirements on Bring-Your-Own-Key. Few vendors provide it, but it’s changing.

Tools reflect the Organisation

- **A CNAPP** is very user friendly and we use it as the quick win solution, but our security teams still are:
  - split (not a single team checking all signals)
  - have most of their clients in the Data Centre

  ... thus we are switching to dedicated, usually agent-based, tools for vulnerability assessment and EDR.

- **Identity** is essential, but not covered in this presentation

More Learnings

#1 Start with security observability and financial responsibility

#2 We did wait a lot to officialise a cloud security policy. It would been easier and safer to start with a practical benchmark and iterate over it.

#3 Start from industry benchmarks (but they do have their blind spots)

#4 Keep custom tool development to a minimum. Rework your plan to align with product roadmap

#5 Big customers have leverage on tool vendors. A request that is useful for other customers might be implemented quickly

#6 Cloud Provider security tools are easier to deploy, but not always sufficient.

Thank you

European Commission