

Our Journey to Shift-left Security with Infrastructure as Code



Romina Druta
Sr. Cloud and Security Research Engineer

About Visma



We are a **Top 5 software company in Europe**



Wide network
of distributors and partners



No. 1 in Cloud ERP in Europe



We have a **large and diversified** technology stack



We operate across
Europe and Latin America



Visma in numbers



15000+

Engaged employees



1.4M

Customers



€ 2 056M

Revenue in 2022
Value created for **society** in 2022



5000+

Developers



265+

Locations - strong local presence
We are where you are



11M & 22M

Payslips
e-invoices
running through Visma's systems
every month



300

companies have joined Visma
last decade



Leading in cloud software



€ 1 700M

Cloud revenue 2022



~90% of R&D spend

Cloud solutions are top priority



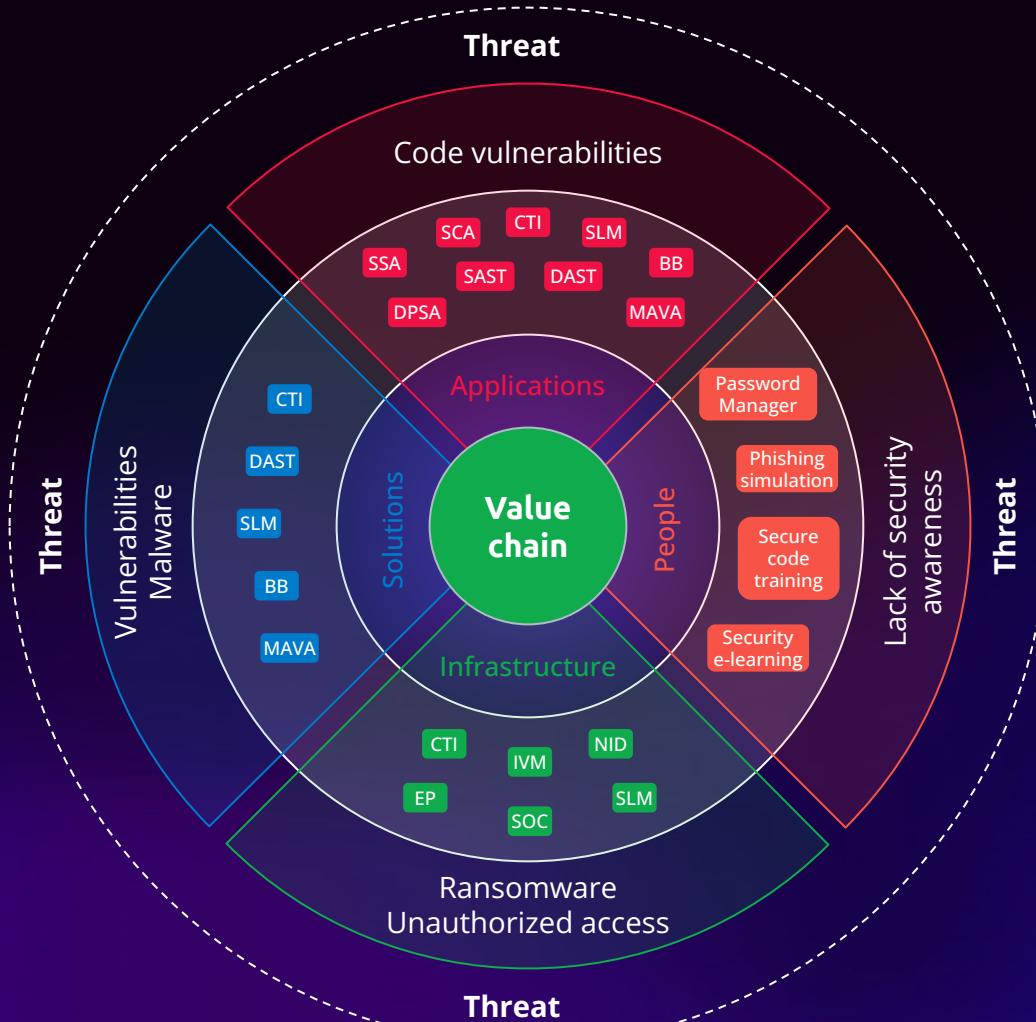
Google Cloud



800 AWS, 800 Azure and 400 GCP

2000 cloud operational accounts

Security Program



Visma Application Security Program



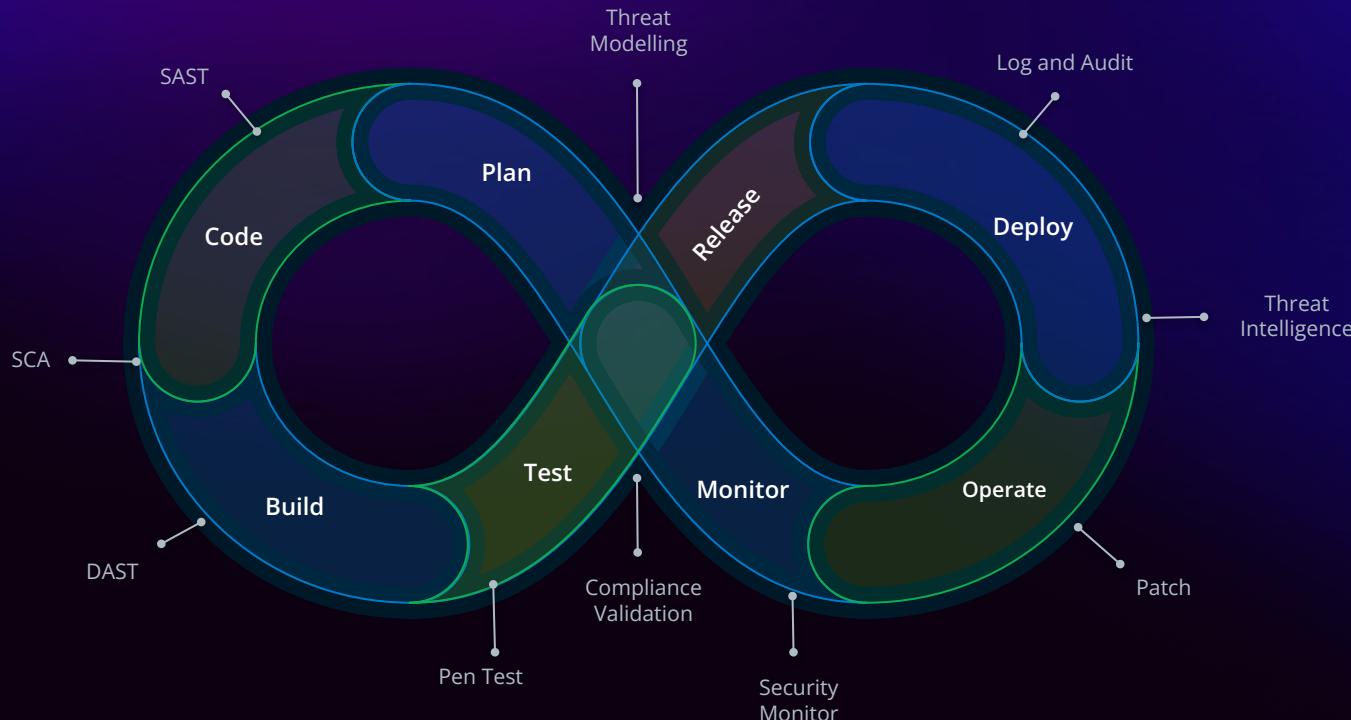
What is Shift-left Security?

Shift-Left Security

- Positions the security process to a point early in the delivery lifecycle
- Educate and train developers on securing the coding practices
- Boost the security of your environment



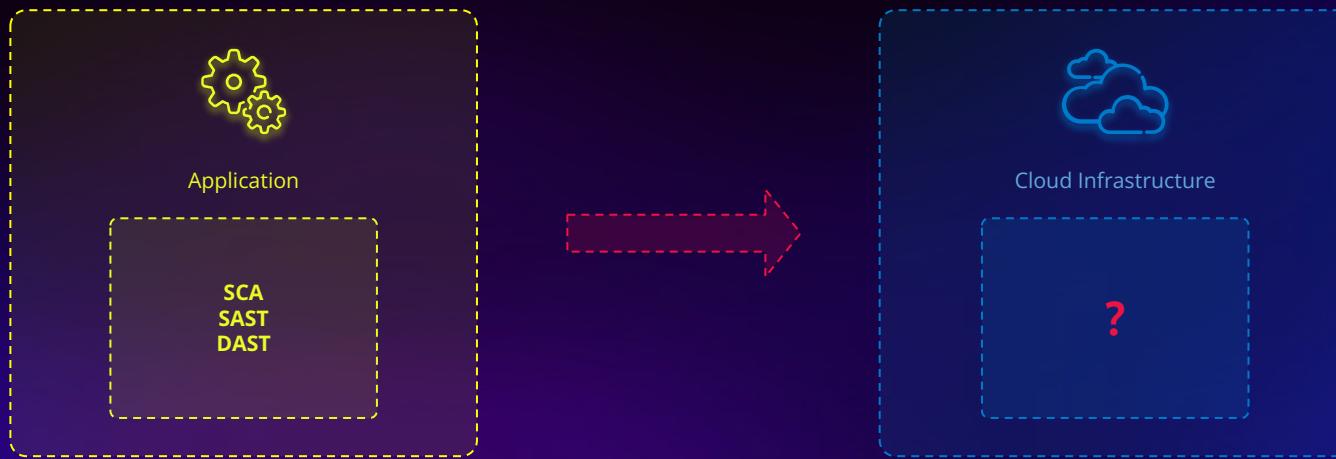
DevSecOps - Application Code



How all started?

Applications are code based but the Cloud Infrastructure **started to be code based** as well

What do we have in place to secure the Cloud Infrastructure code?



Cloud Security Risks with IaC

- Lack or poor configuration of **IAM policies**
- **Network misconfigurations**
- **Secrets management**
- **Publicly exposed** resources
 - Storages
 - Databases
 - Virtual machines
 - Kubernetes Control Plane Api

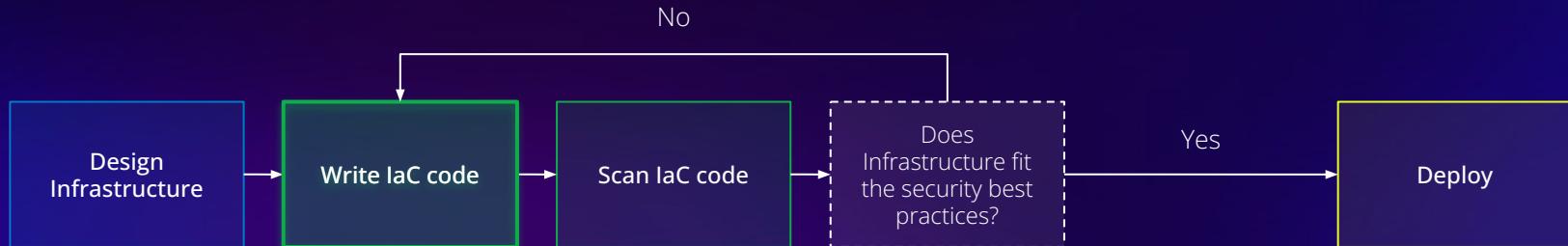


Shift left with IaC Scan

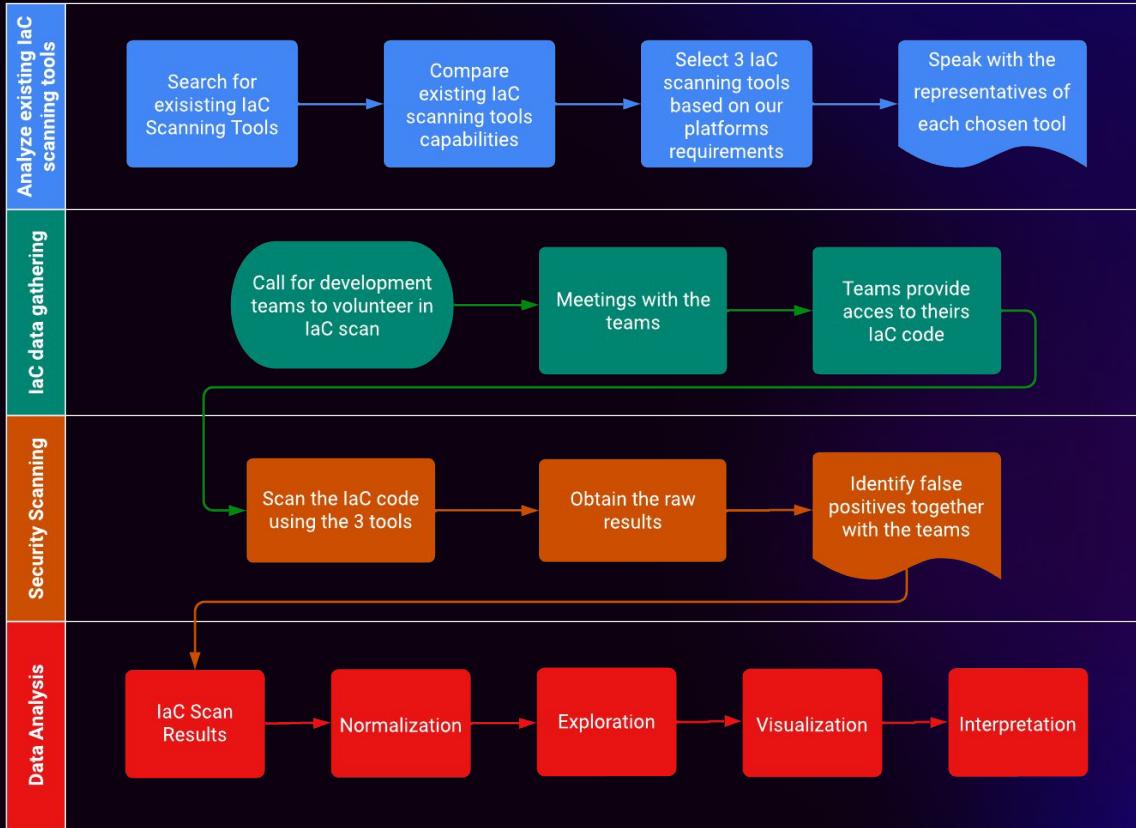
- ✓ **Automate** Infrastructure provisioning
 - Manage everything through code
- ✓ Reduce the risk by adopting **shift-left security**
 - Detect miss-configurations and vulnerabilities



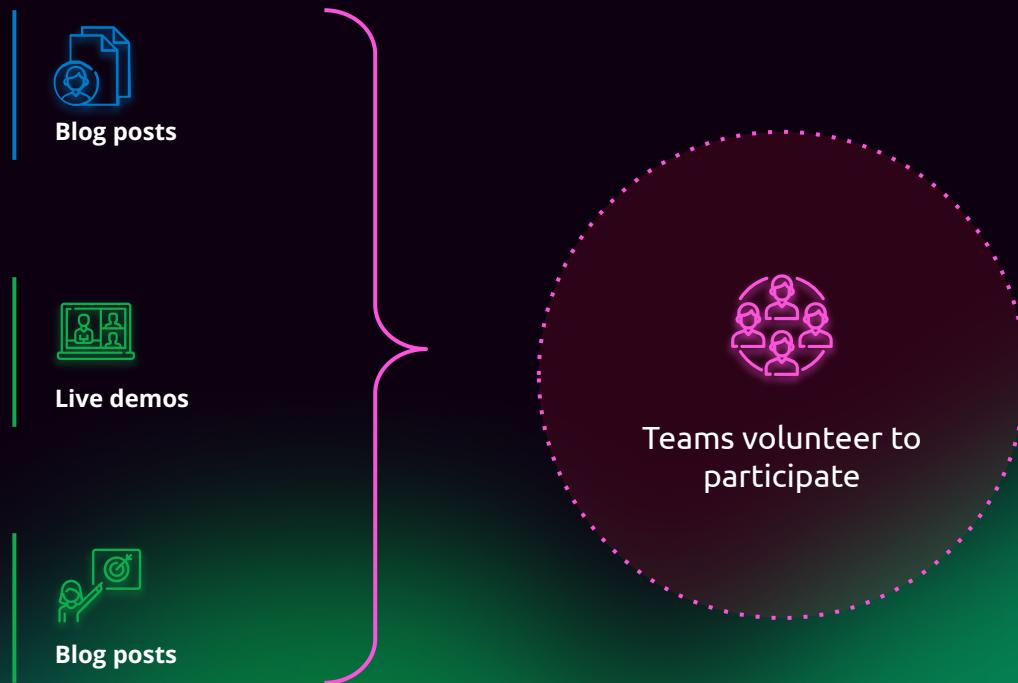
Our Goal → find a tool that can be adopted by all teams in our Company



Our Research Methodology



Involving the teams



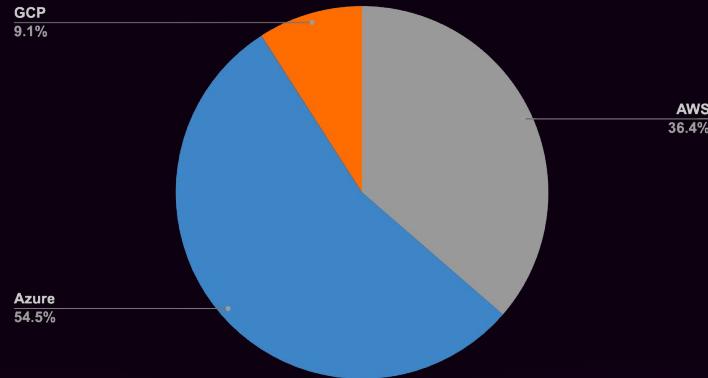
Tools evaluation

- ★ Ease of installation and configuration
- ★ Usability/User-friendliness
- ★ Type of policies
- ★ Reports readability
- ★ Documentation
- ★ Findings(e.g. Vulnerabilities, false positives)
- ★ Interoperability (e.g.Platforms integration)



Our case Study

Cloud provider

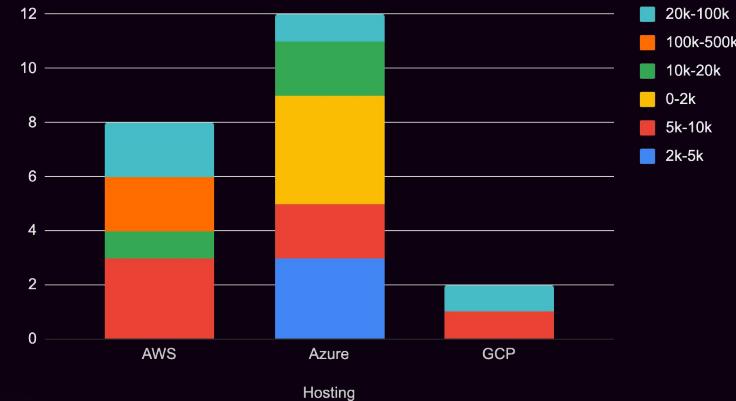


22

teams

- Azure - 12
- GCP - 2
- AWS - 8

Projects size by Cloud Provider



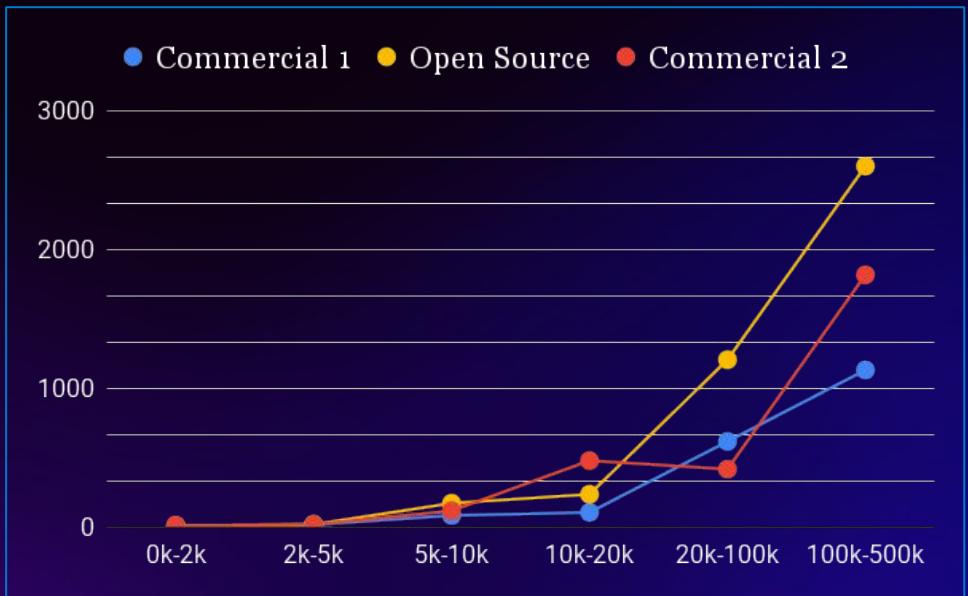
Cloud Provider | Lines of code

Cloud Provider	Lines of code
AWS	761 633
Azure	139 223
GCP	30 524
Total	931 380

Results

→ Distribution of vulnerabilities by project size and tool

- ◆ As project size is bigger the number of vulnerabilities increases
- ◆ Default Configurations - might be prone to vulnerabilities
- ◆ Practitioners need more knowledge for new cloud services → Early adopters of new trends (*K8s in general*) had misconfigurations



Common Issues across Providers

→ Publicly Exposed resources

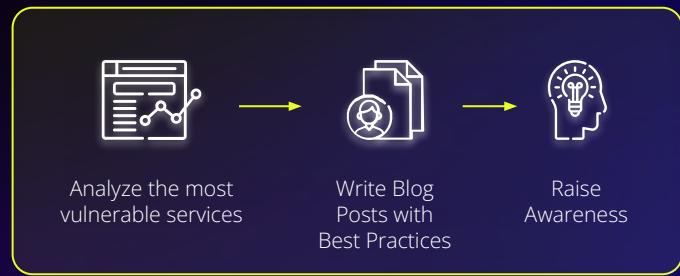
- ◆ Storage Accounts
- ◆ Virtual Machines
- ◆ Kubernetes Clusters

→ Encryption problems

- ◆ Databases
- ◆ Volumes Disks
- ◆ Storages

→ IAM issues

- ◆ Wrongly configured IAM policies
- ◆ Users with wide permissions



What the teams were saying

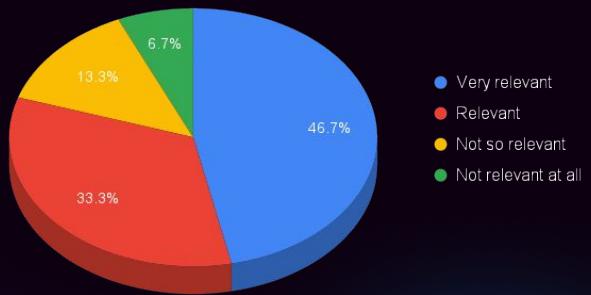
Tools

- Documentation and reports readability are essential
- GUI and Dashboards were important for developers
- Preference for a tool for all security related scans

Experience

- Involving the teams helped them to understand better their infrastructure
- Discussions with the specialists were appreciated
- Team members were motivated to adopt IaC scan

How relevant do you think this tool would be when it comes to improving security posture of your Infrastructure?



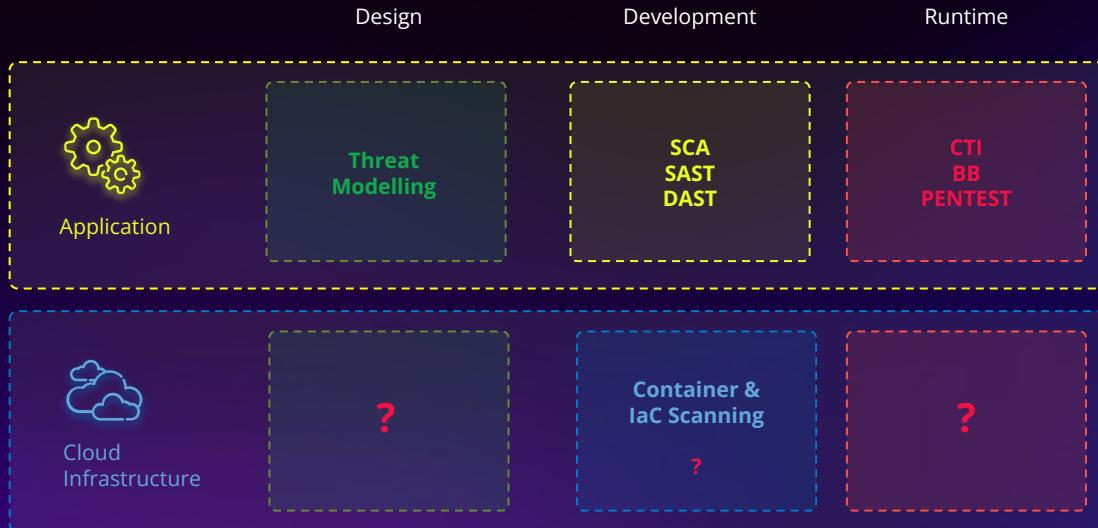
What we have discovered?

- Cloud infrastructure partially provisioned using IaC
- Teams prioritize code security while ignoring cloud security runtime(workload protection and data protection)
- IaC scanning is not applicable if we have drift.

IaC scanning is not enough
We were missing other pieces in the puzzle



What more are we missing?

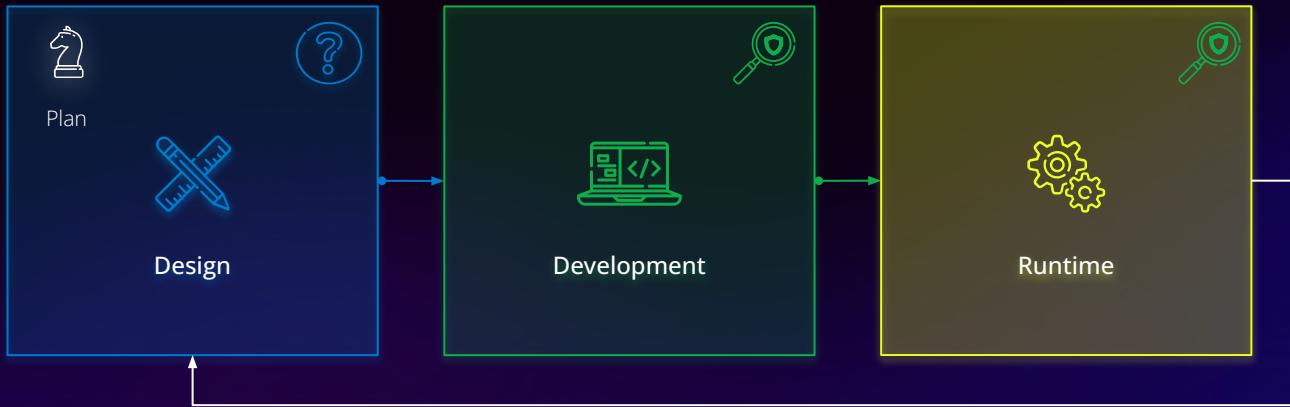


Addressing Full Cloud Security

- CSPM - Cloud Security Posture Management
 - Workload Misconfigurations, Network Misconfigurations,
 - Logging and Monitoring , Best Practices
- CIEM- Cloud Identity and Entitlement Management
 - IAM Misconfigurations
 - Authentication
- CWPP - Cloud Workload Protection Platform
 - System Integrity, Malicious Activity
 - Malware,Vulnerable components
- DSPM - Data Security Protection Platform
 - Data at Risk
 - Data Protection
- API Security
 - Endpoints at risk



Improve our Security by Design Process

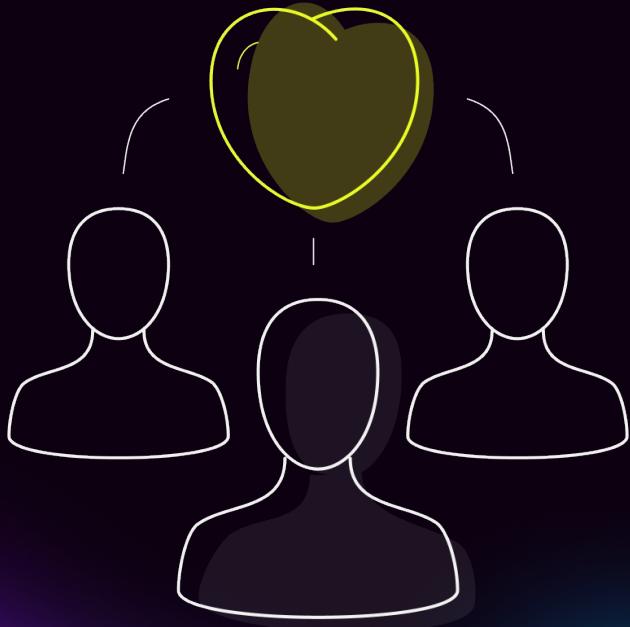


Some security findings can be eliminated during Threat Modelling sessions

- What we discover at the coding phase?
- What we discover with scanning at the runtime?
- What can be prevented at the design phase?

Lessons learned

- Not blaming teams having security issues encourages trust and openness
- Involving teams in choosing the right tool motivates them in adopting new technologies
- Discussing the findings with the teams increases the security knowledge
- We validate the tools, we train the people and they became the ambassadors on the subject



Conclusion



Cloud Security → **shared responsibility**

Shift-left with IaC Scan → **one step in your defense line**

Teams involvement → **elevates security awareness and knowledge**

Questions?

The floor is open to discussions



Visma
Security Program



**Entrepreneurial
Responsible
Dedicated
Inclusive**

Make progress happen

