Visma
Security Program

Our Journey to Shift-left Security with **Infrastructure as Code**

Romina Druta
Sr. Cloud and Security Research Engineer

VISMA

About Visma

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

No. 1 in Cloud ERP in Europe

Wide network
of distributors and partners

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

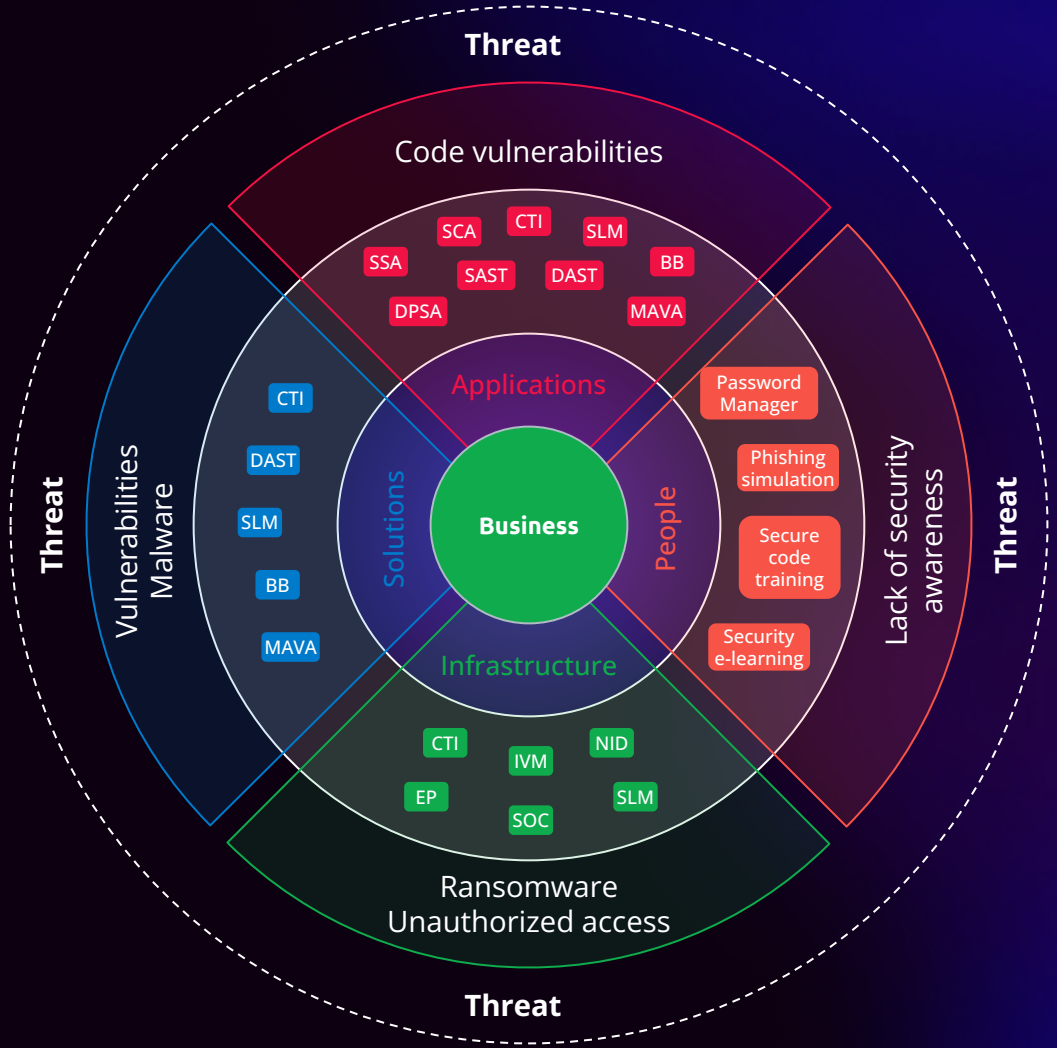
Leading in cloud software

€ 1 700M
Cloud revenue 2022

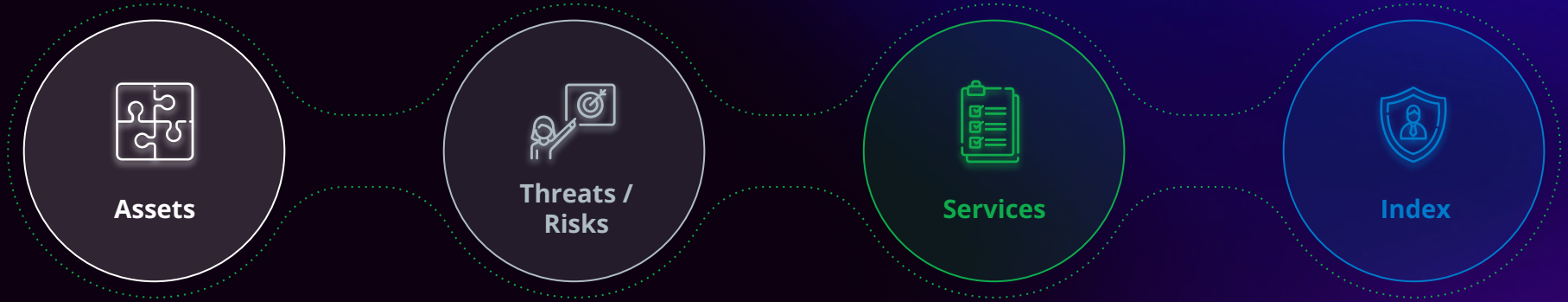
~90% of R&D spend
Cloud solutions are top priority

800 AWS, 800 Azure and 400 GCP
2000 cloud operational accounts

VSP


Threat
Code vulnerabilities
SCA
CTI
SLM
SSA
SAST
DAST
BB
DPSA
MAVA
Applications
Threat
Vulnerabilities
Malware
CTI
DAST
SLM
BB
MAVA
Solutions
Business
People
Password Manager
Phishing simulation
Secure code training
Security e-learning
Lack of security awareness
Threat
Infrastructure
CTI
IVM
NID
EP
SLM
SOC
Ransomware
Unauthorized access
Threat

Visma Application Security Program



Applications

Software application that we write and control

Risk of data breach due to potential code vulnerabilities

Shift-Left Security

DPSA	Data Protection Self-Assessment
SSA	Security Self-Assessment
SAST	Static Application Security Test
SCA	Software Composition Analysis
DAST	Dynamic Application Security Test
PENTEST	Penetration Test
CTI	Cyber Threat Intelligence
BB	Bug Bounty
RD	Responsible Disclosure

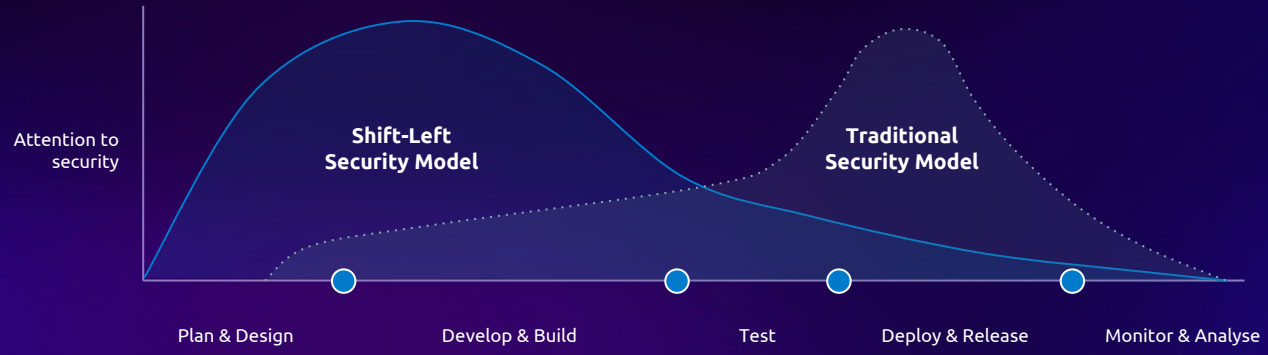
What security tier should be in place?

How well are we covered for the risks?

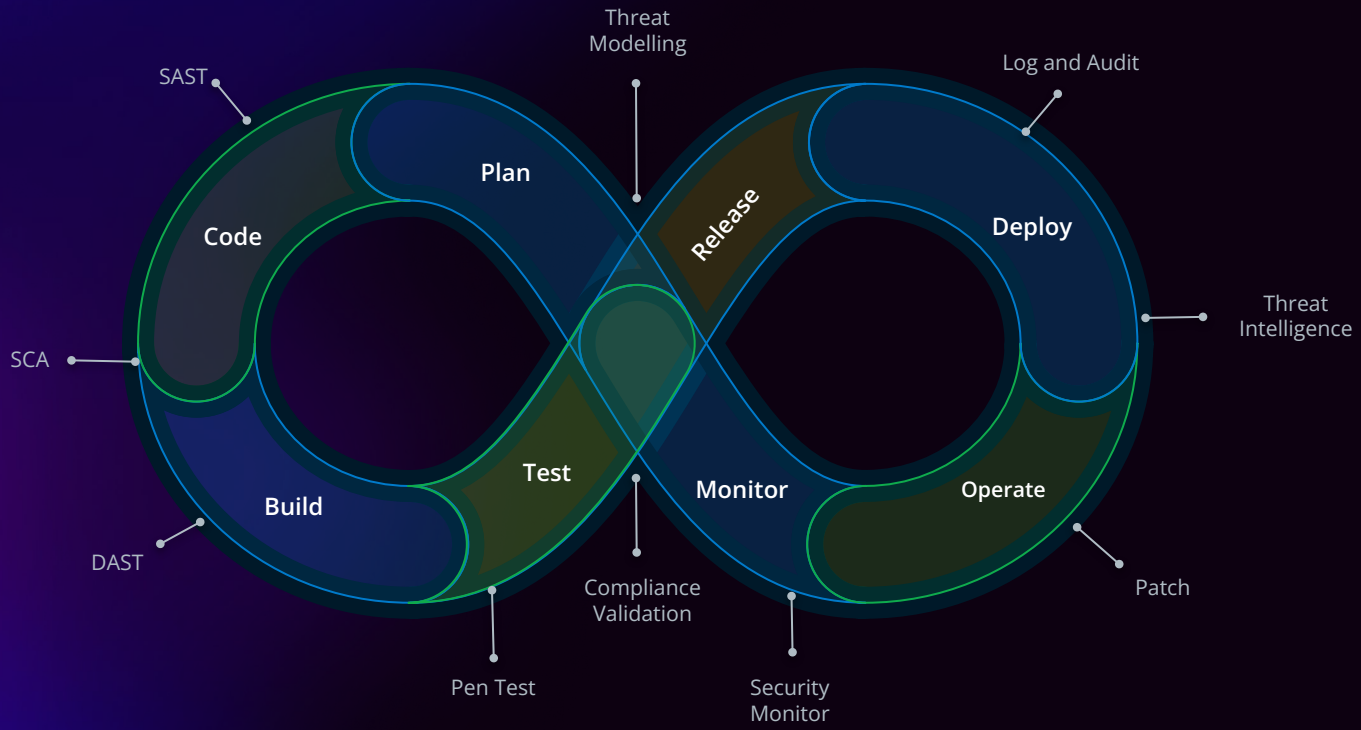
What is Shift-left Security?

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



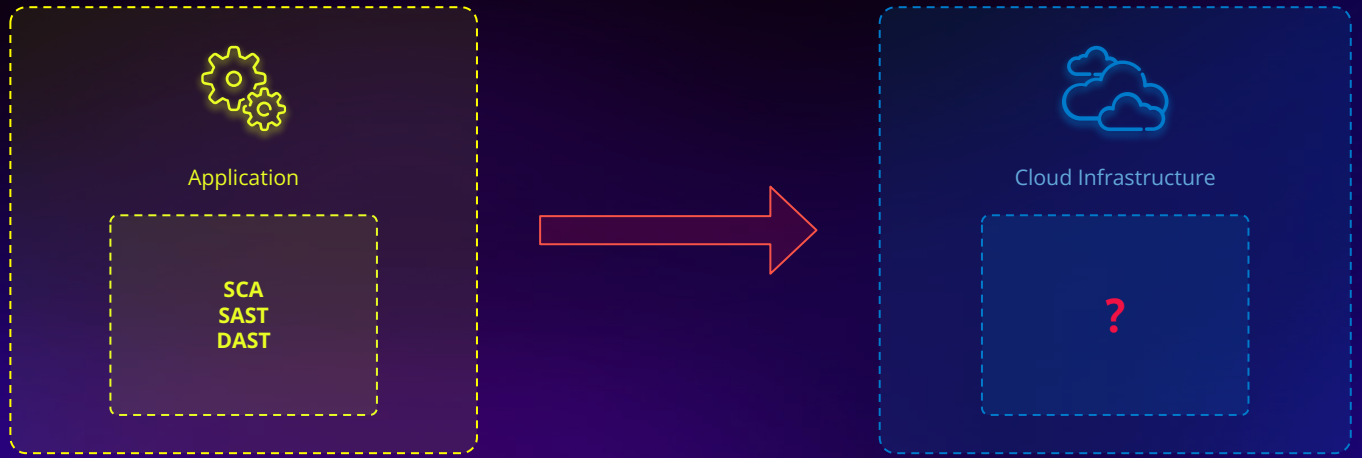
DevSecOps - Application Code



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?

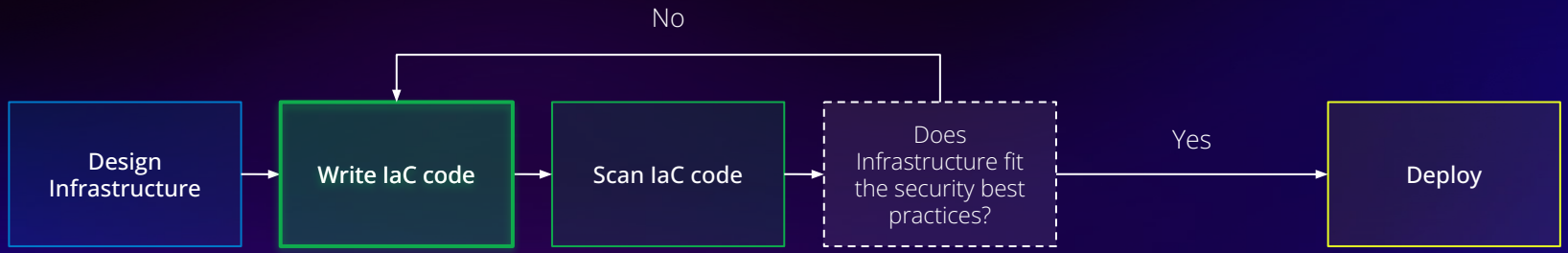


Cloud Security Risks with IaC

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

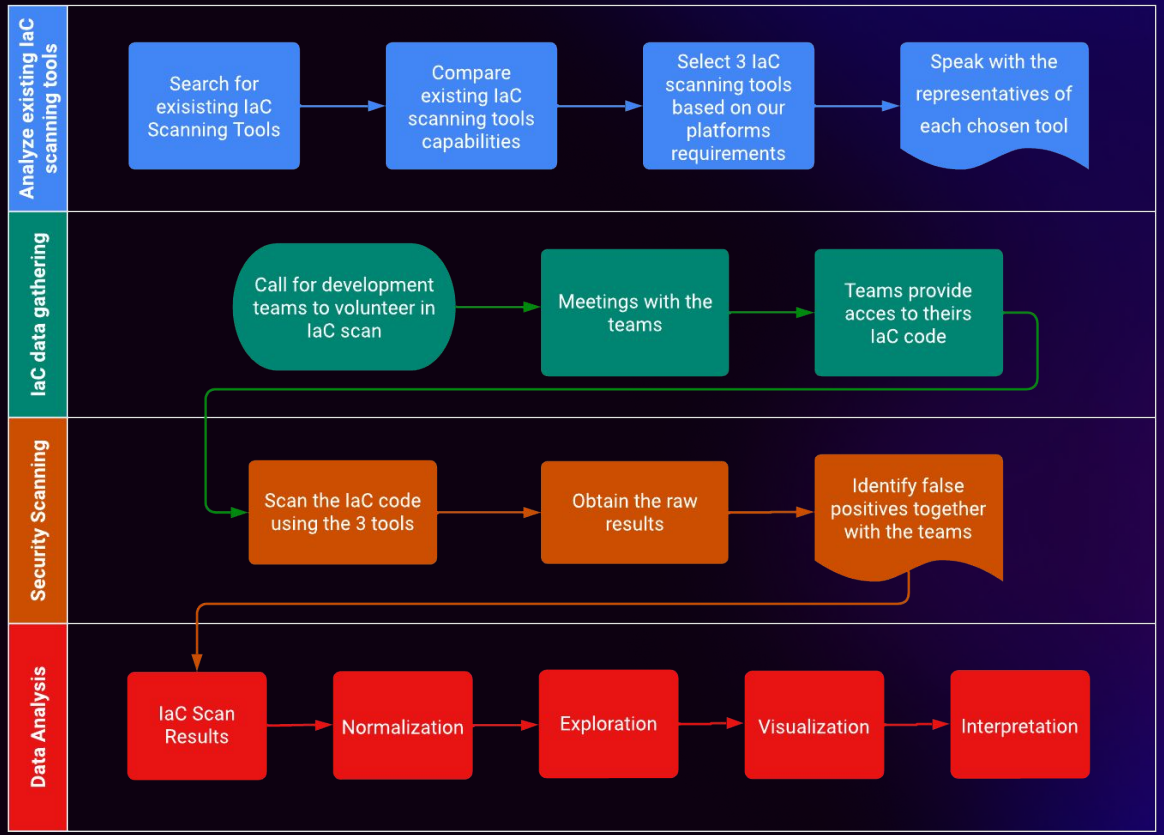
Shift left with IaC Scan

- ✔ **Automate** Infrastructure provisioning
- ✔ Reduce the risk by adopting **shift-left security**
  - Detect miss-configurations and vulnerabilities



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

Our Research Methodology



Tools evaluation

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

Involving the teams

Blog posts

Live demos

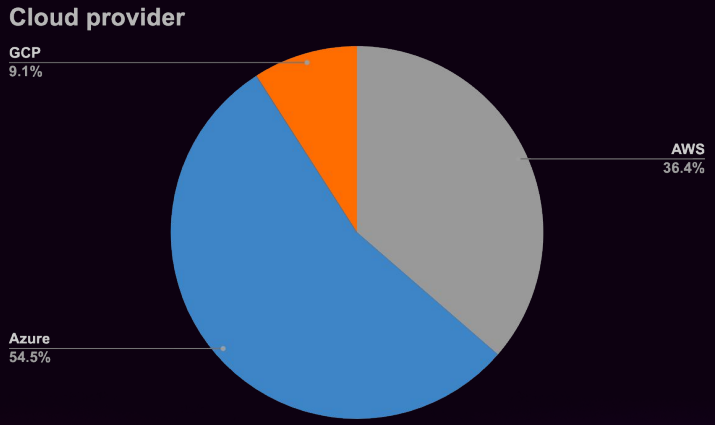
Guild channels

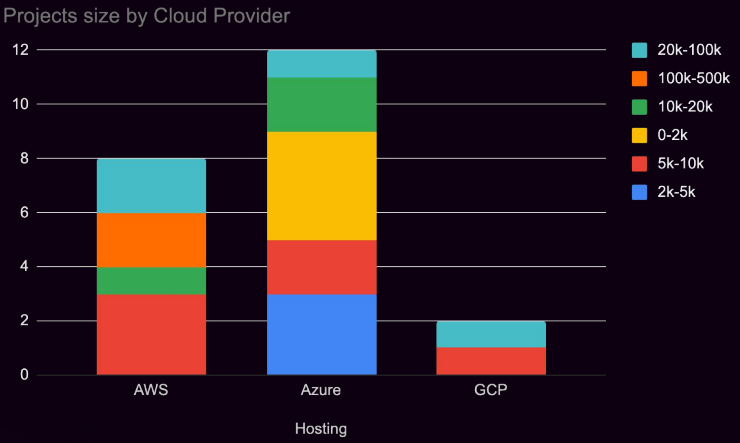
Teams volunteer to participate

Identify False positives

Feedback Forms

Our case Study





22
teams

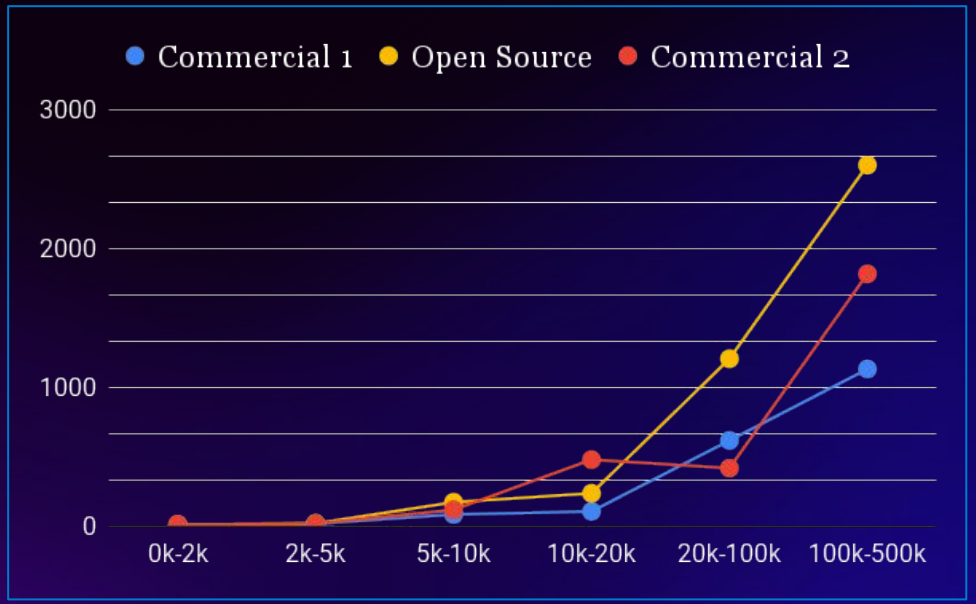
- Azure - **12**
- GCP - **2**
- AWS - **8**

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
- Tools perform different in function of the IaC file type
- Different coverage across cloud platforms



Common Issues across Providers

Publicly Exposed resources

- Storage Accounts
- Virtual Machines
- Kubernetes Clusters

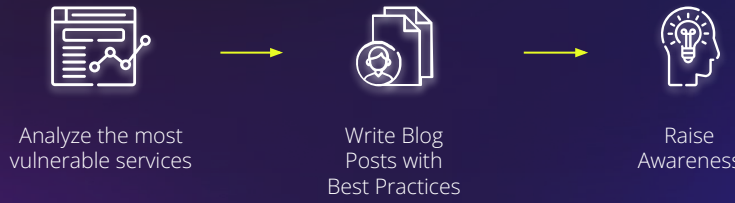
IAM issues

- Wrongly configured IAM policies
- Users with wide permissions

Encryption problems

- Databases
- Volumes Disks
- Storages

- Default Configurations - might be prone to vulnerabilities
- Practitioners need more knowledge for new cloud services
- **No hard-coded secrets** → result of security awareness



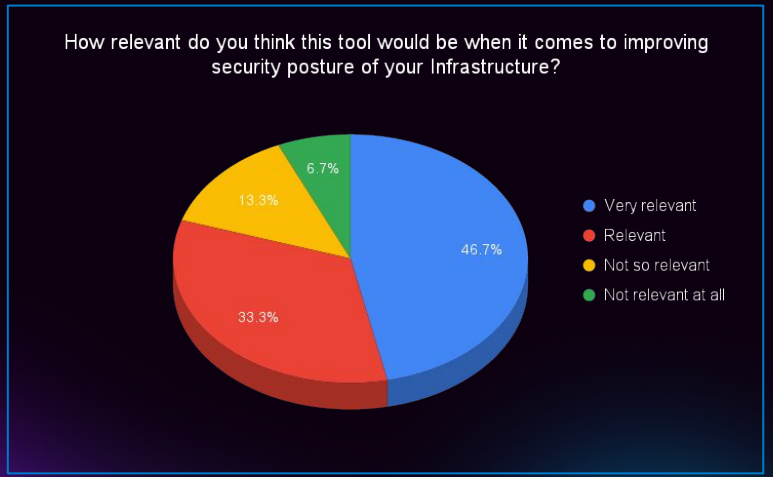
What the teams were saying

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 security specialists were appreciated
- Team members were motivated to adopt IaC scan

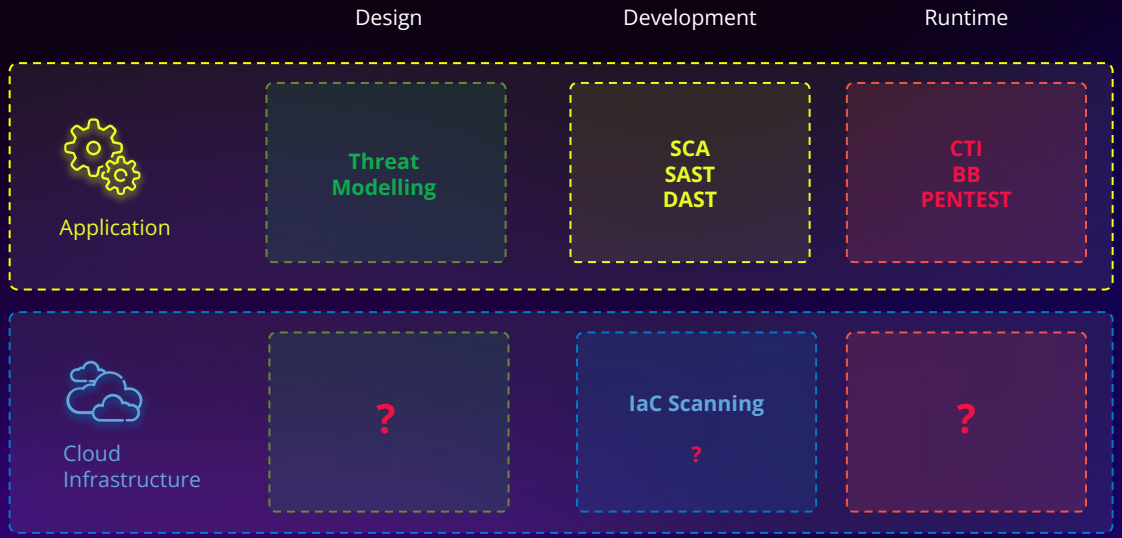


What we have discovered?

- ➔ Cloud infrastructure partially provisioned using IaC
- ➔ Infrastructure created with bash/powershell scripts
- ➔ IaC scanning is not applicable if we have drift
- ➔ Teams prioritize code security while ignoring cloud security runtime *(workload protection and data protection)*

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

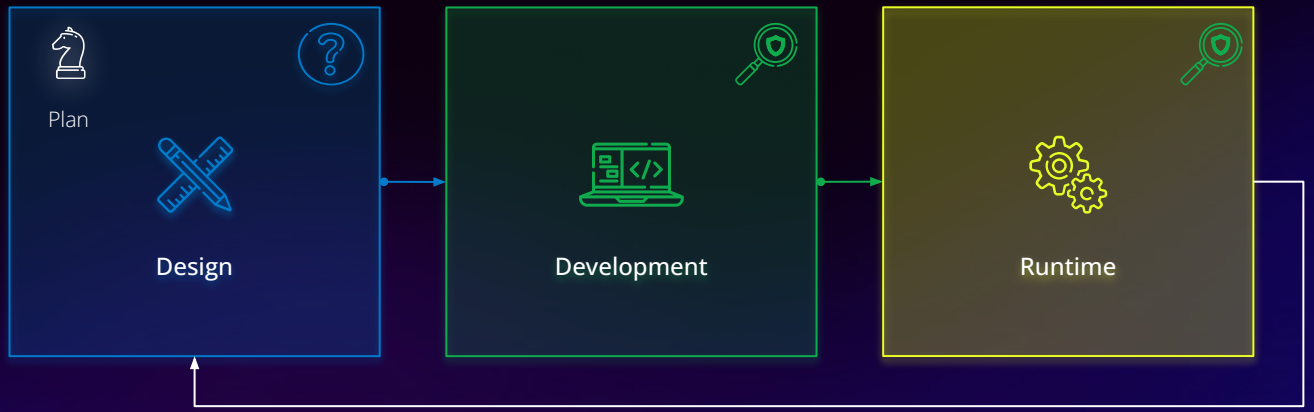
What more are we missing?



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

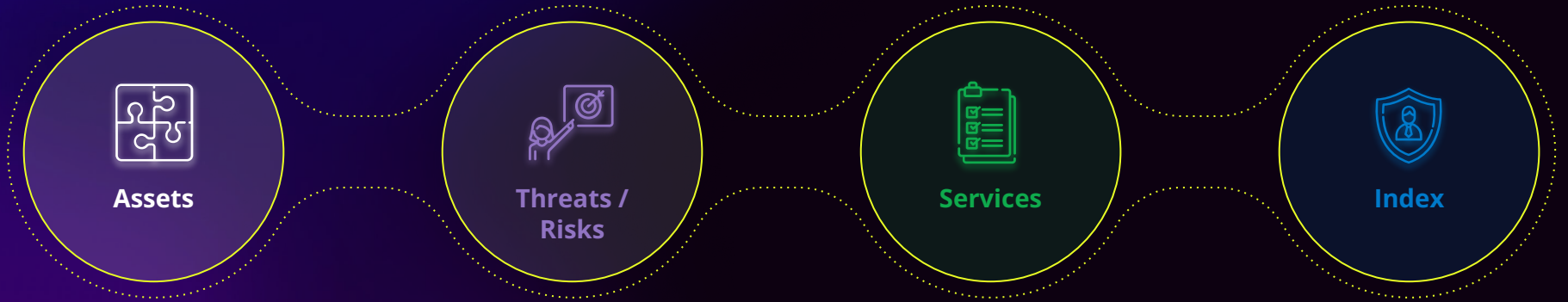
Improve our Security by Design Process



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?

Cloud Infrastructure Security



Cloud Assets

Risk of incident due to security misconfigurations

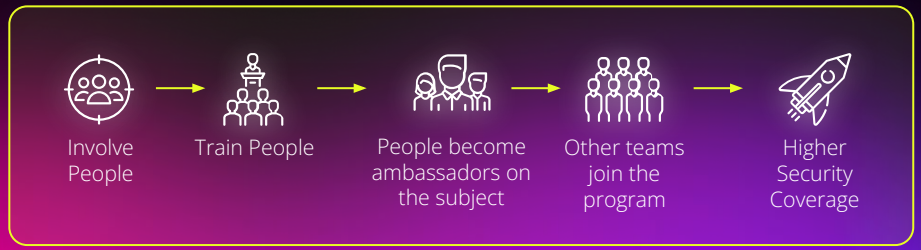
- IaC Scan
- CWPP
- CIEM
- ...

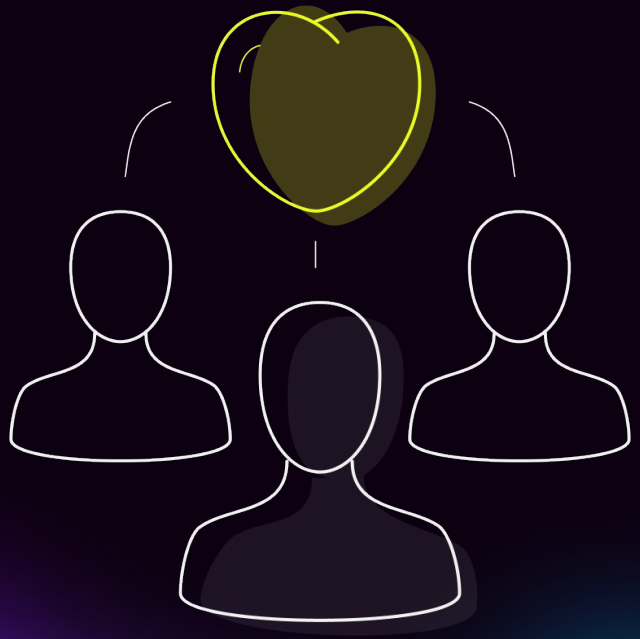
What security tier should be in place?

How well are we covered for the risks?

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

VISMA