The RISER Project

RISER: RISC-V for cloud services

Cloud Application Security

Secure SDLC

Pavel Sorokin @ CloudSigma

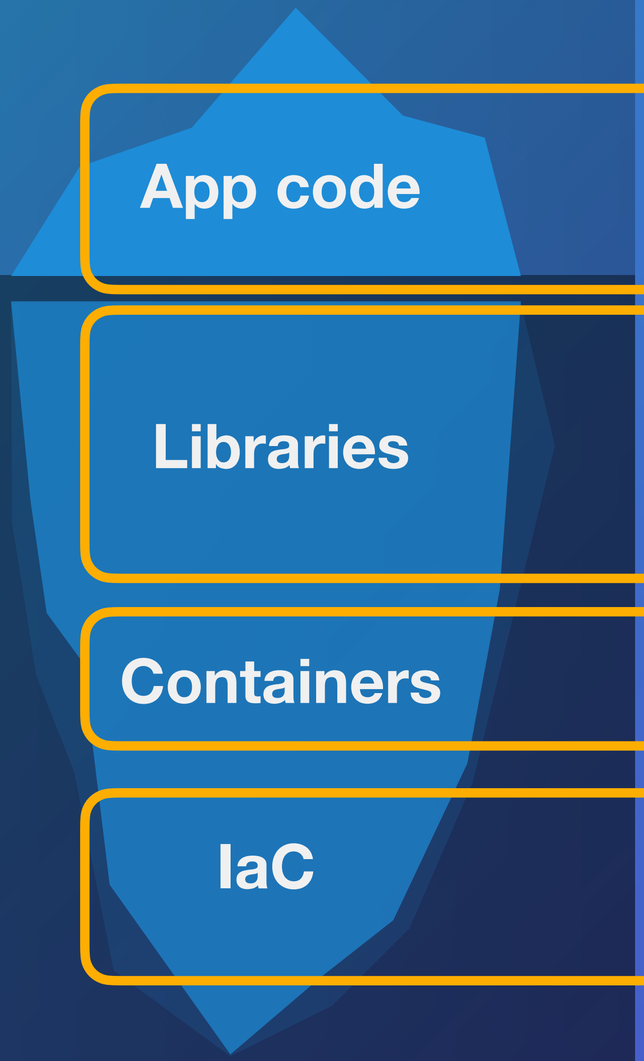
Riser Project Webinar, 08.11.2023

Agenda

- Modern application risk profile
- Secure SDLC
- Best practices
- Takeaways

Why does bringing Security into cloud-based applications matter?

Modern application risk profile



App code

- **10-20%** of code is custom
- code vulnerabilities

Libraries

- **80-90%** of codebase is open source
- known vulnerabilities
- **80%** of vulnerabilities found in transitive dependencies

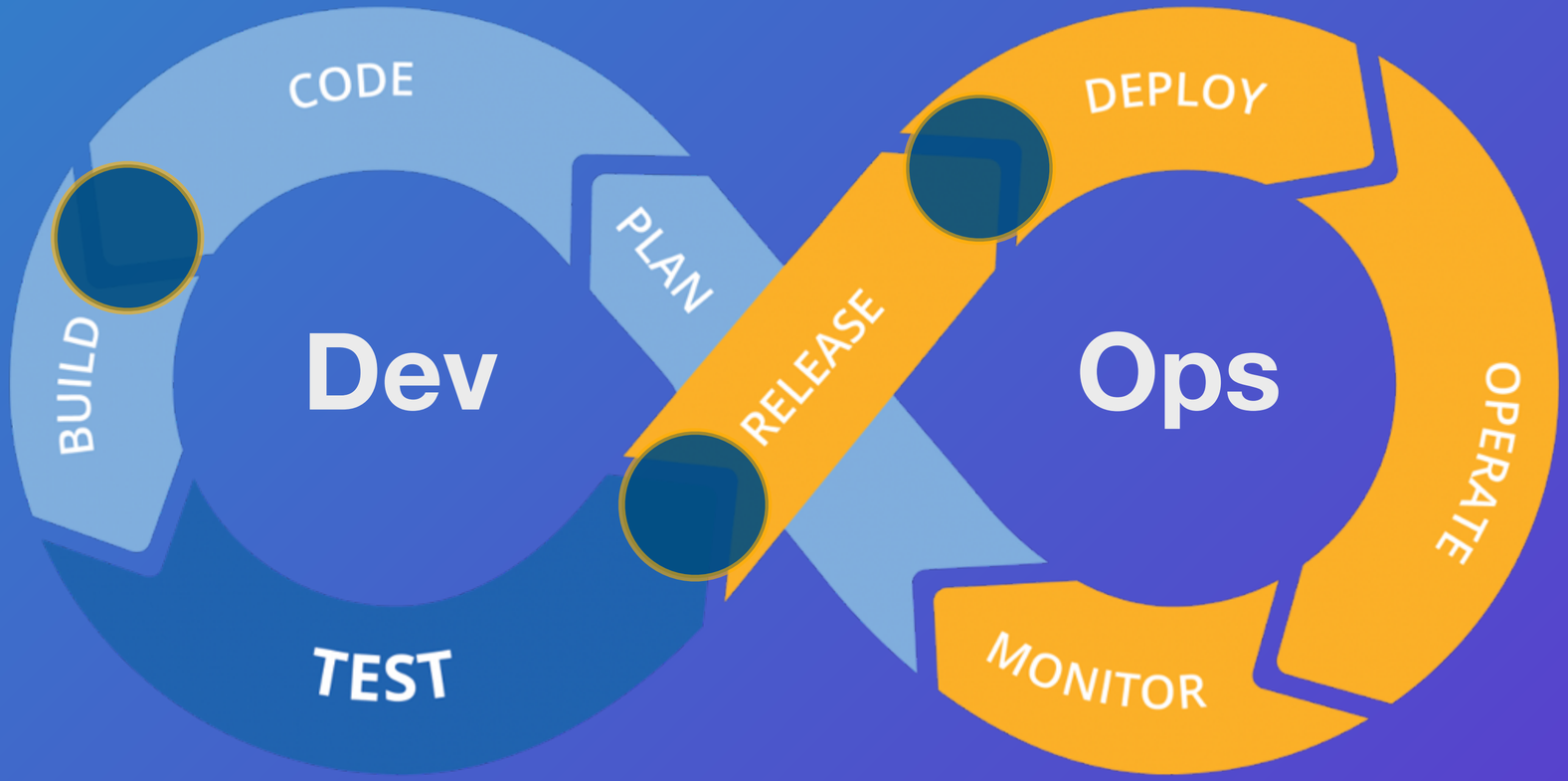
Containers

- Linux packages inherited from public sources

IaC

- network access, storage, servers
- #1 cloud vulnerability is misconfiguration [NSA]

Secure SDLC



security gates

Static Application Security Testing (SAST)

- focus on code
- early in development
- no test cases required
- no execution required
- easy automation

Software Composition Analysis (SCA)

- vulnerabilities in open source dependencies
- licence compliance risks
- unmaintained open source packages

Container Security

- base image scans
- remediation upgrades

Infrastructure as Code (IaC)

- principle of least privilege
- network segmentation
- encryption of data in-transit and at-rest

Best practices

- educate your developers
- maintain a growth mindset
- implement other initiatives (DevOps, SecDevOps)
- tackle the bigger problems first

Takeaways

- integrate security early
- automate and identify actionable fixes
- check and improve your security posture regularly

Demo

The RISER Project

RISER: RISC-V for cloud services

Develop fast.
Stay secure.

Acknowledgment:
RISER is funded under the Horizon Europe proposal call on
“Digital and emerging technologies for competitiveness and fit for the green deal”.

www.riser-project.eu

The RISER Project

RISER: RISC-V for cloud services

Thank you!

Acknowledgment:
RISER is funded under the Horizon Europe proposal call on
“Digital and emerging technologies for competitiveness and fit for the green deal”.

www.riser-project.eu