An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps

Nora Tomas, Jingyue Li, Huang Huang
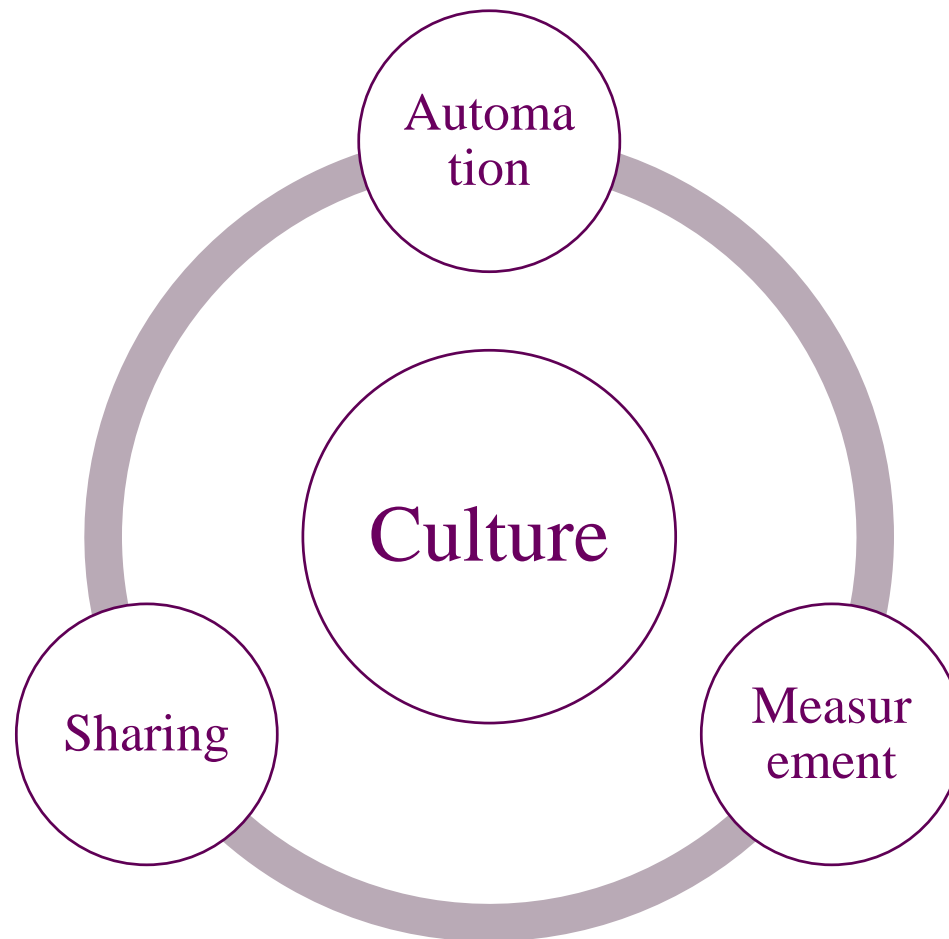
Speaker: Huang Huang
2019.06.04
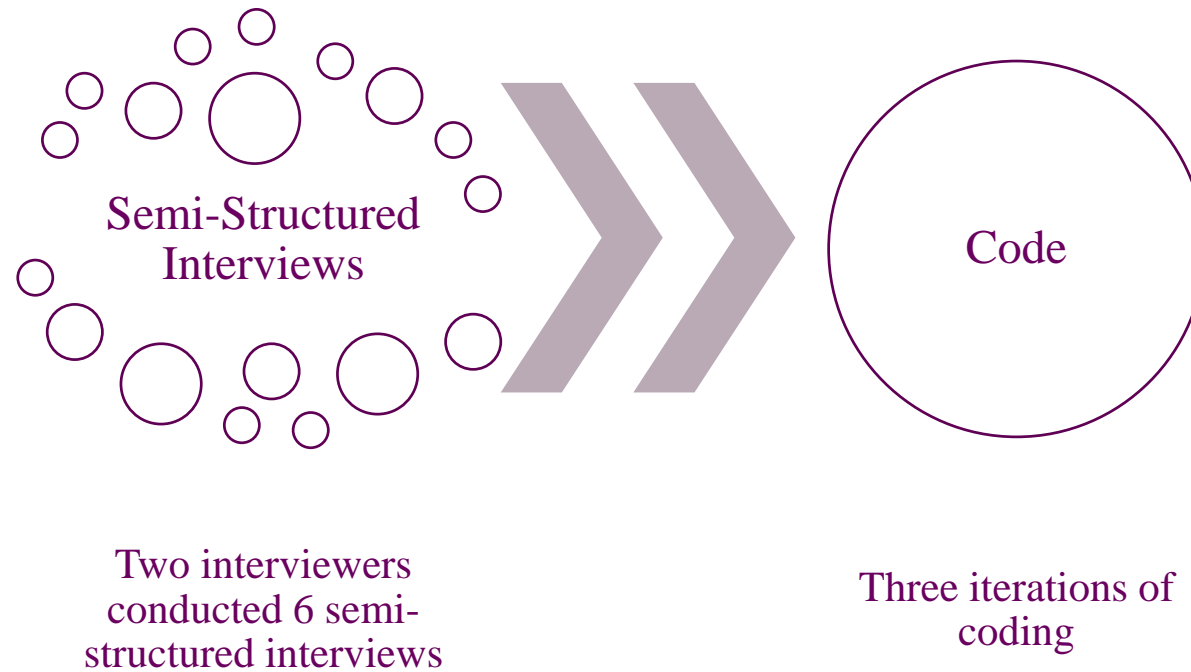
CONTENTS

➢ Background

➢ Methods

➢ Results

➢ Discussion

➢ Conclusion and Future Work

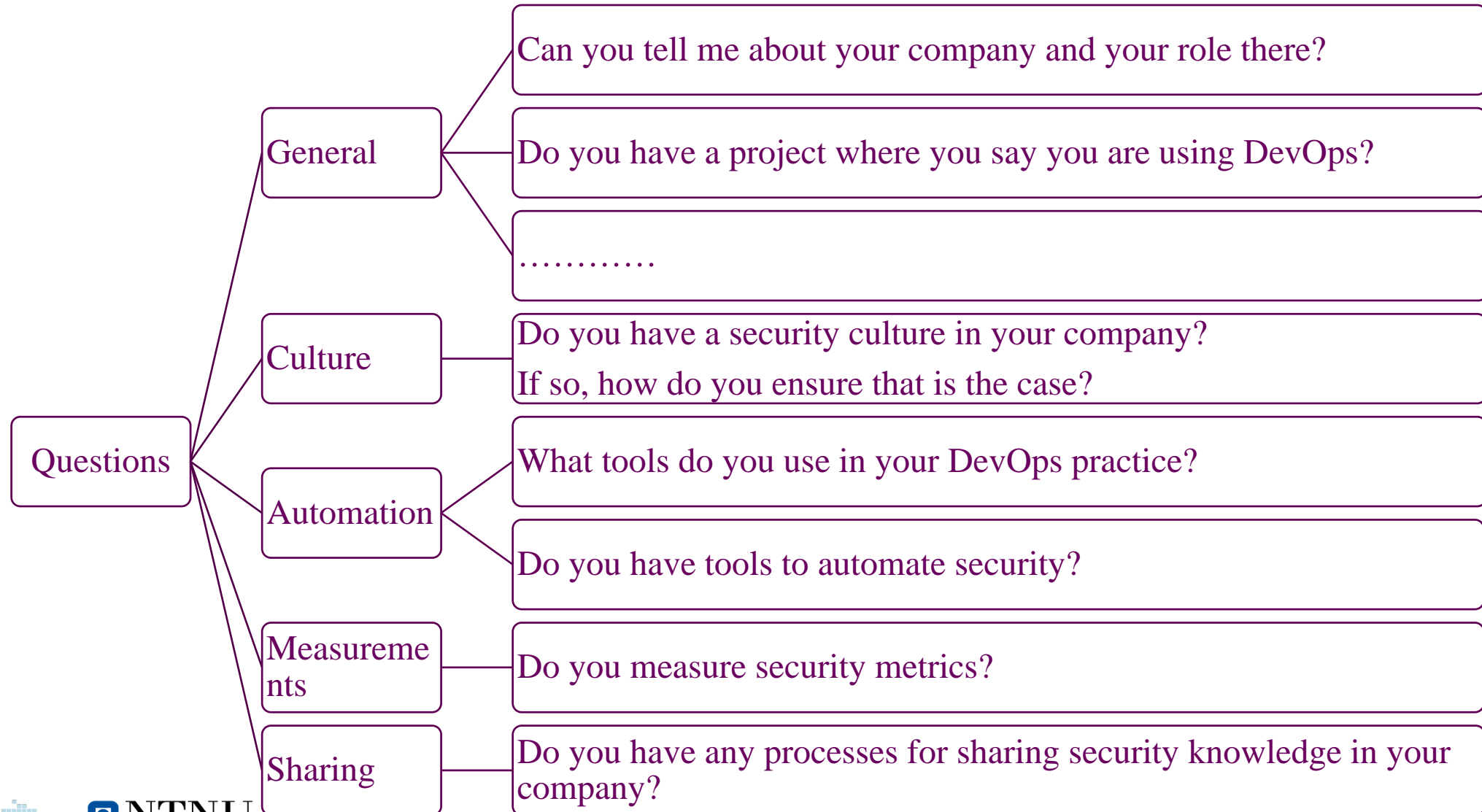# Background – CAMS of DevOps

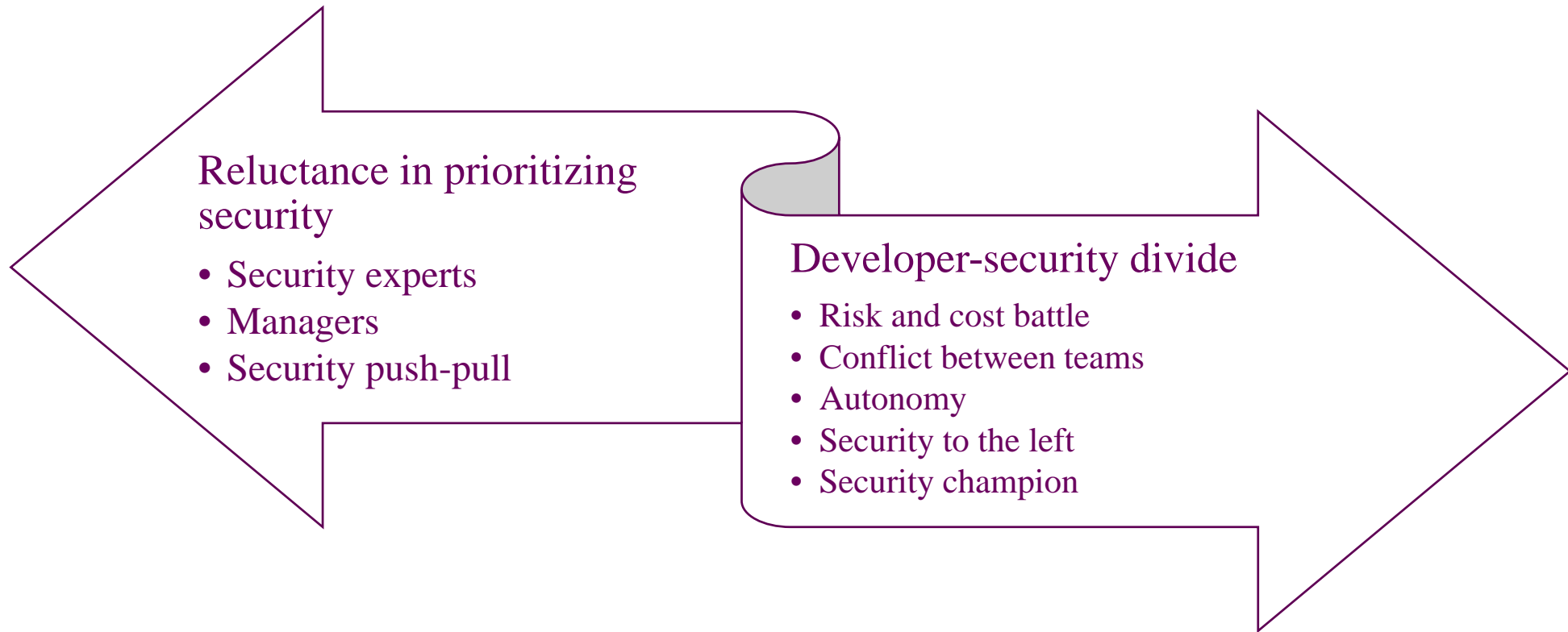# Methods – Industrial Interviews

Semi-Structured Interviews

Code

Two interviewers conducted 6 semi-structured interviews

Three iterations of coding

Methods – Industrial Interviews

INTERVIEW SUBJECT DETAILS

	Role	No. of Employees	Company Product	Company Type
Subject A	Platform Tech Lead	200	SaaS for Smart Cities	Private
Subject B	Software Engineer	11000	Software Security Services	Private
Subject C	Software Engineer	1300	Consulting	Private, but in a public sector project
Subject D	Software Engineer	30	Platform for Web Sites	Private
Subject E	Software/Data Engineer	40	Mobile App	Private
Subject F	Security Architect/ Manager	44000	Consulting	Private

Methods – Industrial Interviews

Questions

General
- Can you tell me about your company and your role there?
- Do you have a project where you say you are using DevOps?
- …………

Culture
- Do you have a security culture in your company? If so, how do you ensure that is the case?

Automation
- What tools do you use in your DevOps practice?
- Do you have tools to automate security?

Measurements
- Do you measure security metrics?

Sharing
- Do you have any processes for sharing security knowledge in your company?

Results – Culture

Reluctance in prioritizing security

- Security experts
- Managers
- Security push-pull

Developer-security divide

- Risk and cost battle
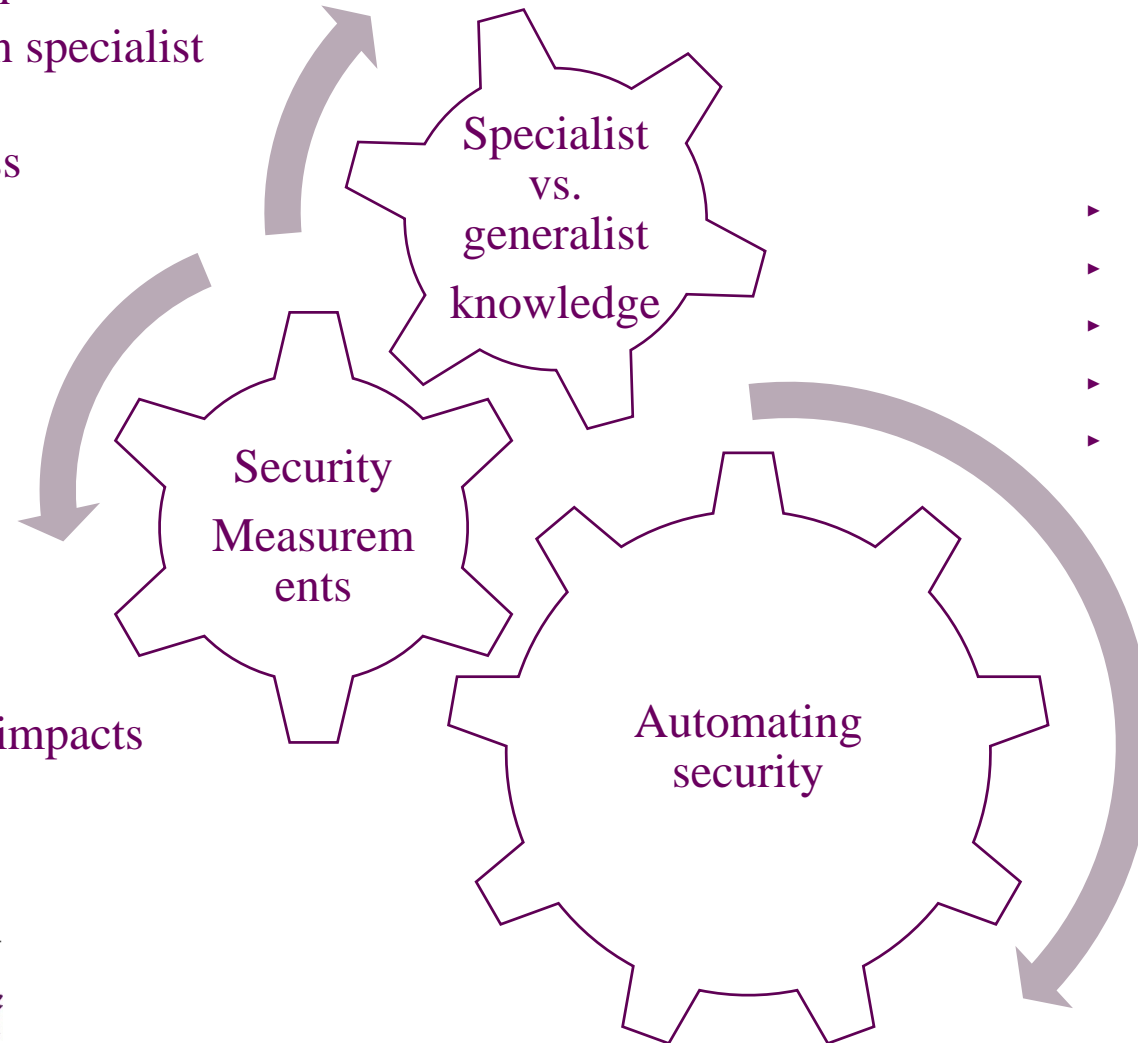- Conflict between teams
- Autonomy
- Security to the left
- Security champion

Results – Automation, Measurement, and Sharing

- ‣ Security education
- ‣ Boundary between specialist and generalist
- ‣ Security awareness

- ‣ Automating legacy system
- ‣ Tool-mindset link
- ‣ Knowledge and training
- ‣ Tool standards
- ‣ Cloud

Specialist vs. generalist knowledge

Security Measurements

Automating security

- ‣ Training
- ‣ Time to repair
- ‣ Vulnerabilities and impacts

Discussion

➢ DevSecOps definition
  • What is the relationship between DevOps and security?
  • What role does DevSecOps play in different companies?

➢ DevSecOps CAMS
  • Security culture is the goal and cornerstone;
  • Knowledge sharing is an interconnecting link;
  • Automation tools are important means in specific tasks.

➢ Comparison with the state of DevOps
  • Security culture is still not applied;
  • Tools are still not enough;
  • Measurements are still too few;
  • Targeted knowledge sharing is less.

Security Tools

Security Training

Security Culture
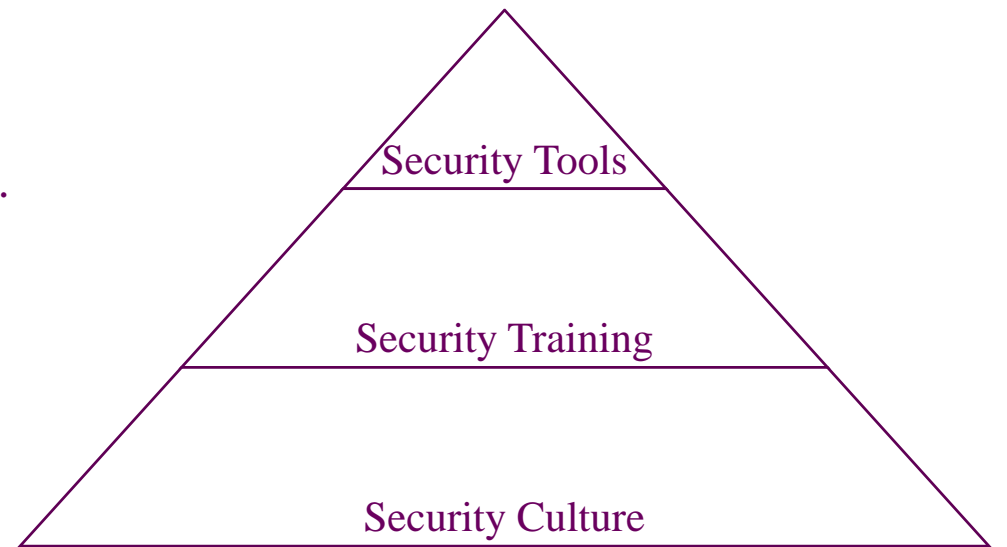
Conclusion and Future Work

- Conclusion:

  - Results of our study reflect the state of the practices of DevSecOps in Norway;

  - We give detailed insights on possible issues and identify some corresponding solutions.

- Future Work

  - More industrial interviews about DevSecOps;

  - A case study on DevSecOps practice;

  - A comparison study on DevSecOps between different cultures.

THANKS

Speaker: Huang Huang
MG1832003@smail.nju.edu.cn
2019.06.04