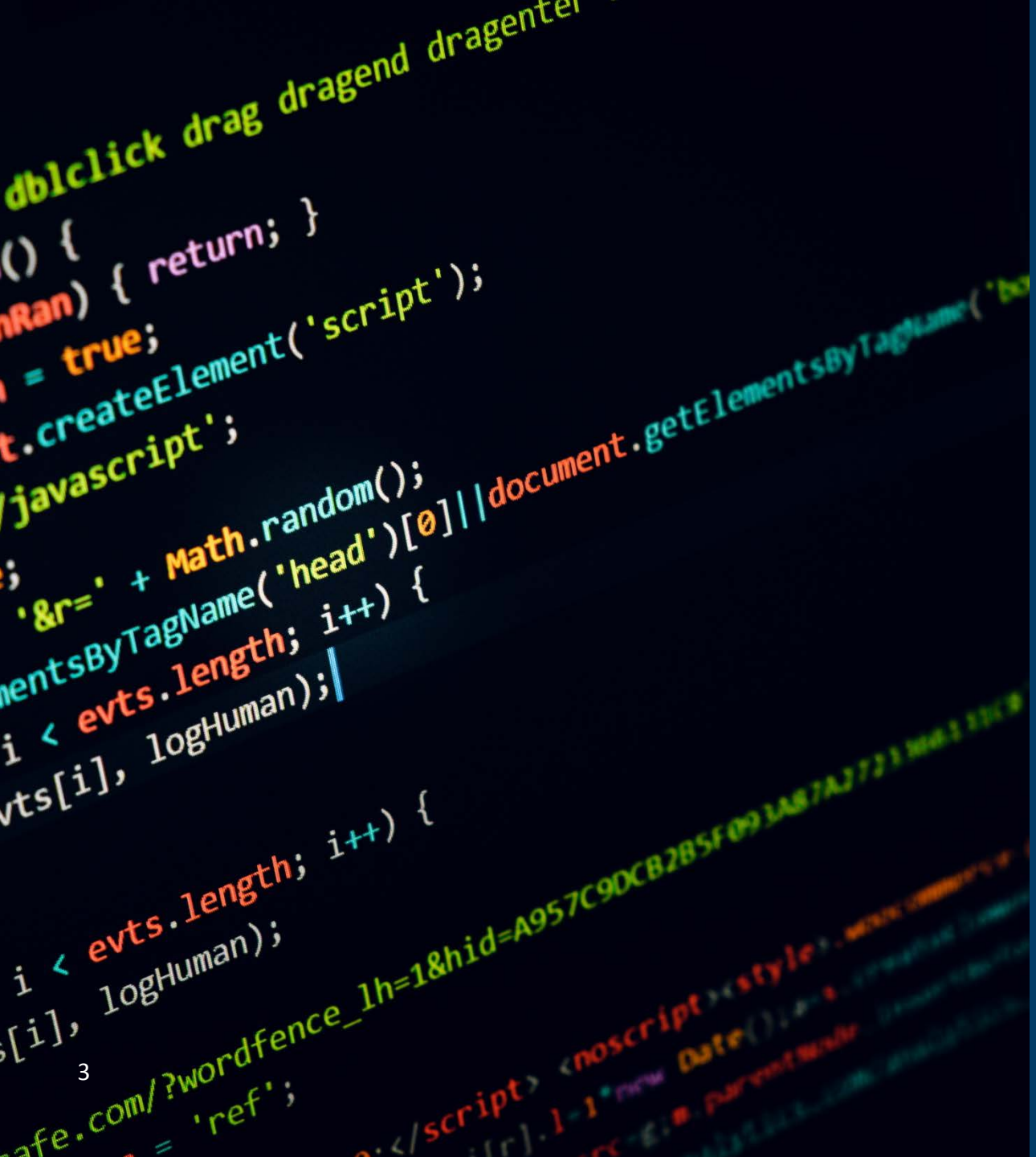
THREAT MODELLING AND AGILE SOFTWARE DEVELOPMENT: IDENTIFIED PRACTICE IN FOUR NORWEGIAN ORGANISATIONS

Karin Bernsmed and Martin Gilje Jaatun

SINTEF Digital, Trondheim, Norway

Agile SW development and security

- The goal of secure software engineering is to create software that keeps performing as intended even when exposed to attacks.
- *Threat modelling* (architectural risk analysis) is one of the most effective activities to improve software security
- However, this practice is not widespread – agile practitioners have little guidance o how to adopt it



Research questions

- What are the main challenges to applying threat modelling in agile software development?
- What are the best practices adopted by agile software development teams?

SINTEF

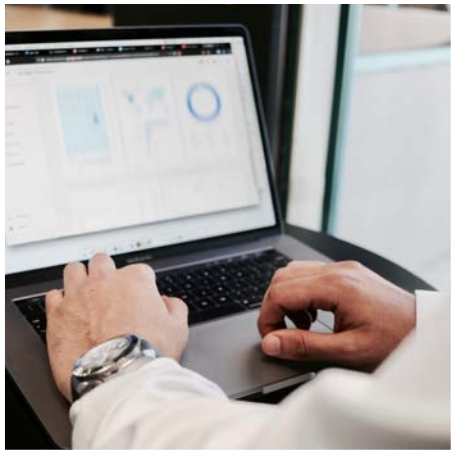
Interviews: industrial context

Organisation A

Organisation B

Organisation C

Organisation D



Interviews: topics

- *What and why?*
- *How and when?*
- *Time spent and definition of done?*
- *Documenting and utilizing the results?*
- *Challenges and benefits?*

Organisation A

"If the goal is to have a secure product, we still have a long way to go. But I don't think we will ever be there. The system is so old, and has been in operation for so long, so to be completely secure it needs to be thrown away and started over […] we need to accept the situation."

SINTEF

Organisation B

"*Developers don’t like tools being forced upon them like a straight-jacket*"

"*The developers don’t have the business perspective..*"

Organisation C

"If you ask a head-hunter whether he can get you a ”DevOp” with security knowledge, he will just laugh.. "

Organisation D

"*Definition of done? You will never be done..*"

Main findings

Observed challenges

- ➢ Lack of motivation
- ➢ Identifying relevant threats
- ➢ Threat modelling is time-consuming
- ➢ Knowing the "definition of done"

Best practices

- ✓ Involving the developers
- ✓ Using checklists and clearly defined processes and routines
- ✓ Triggering the threat modelling activities

Thank you

SINTEF

Technology for a better society