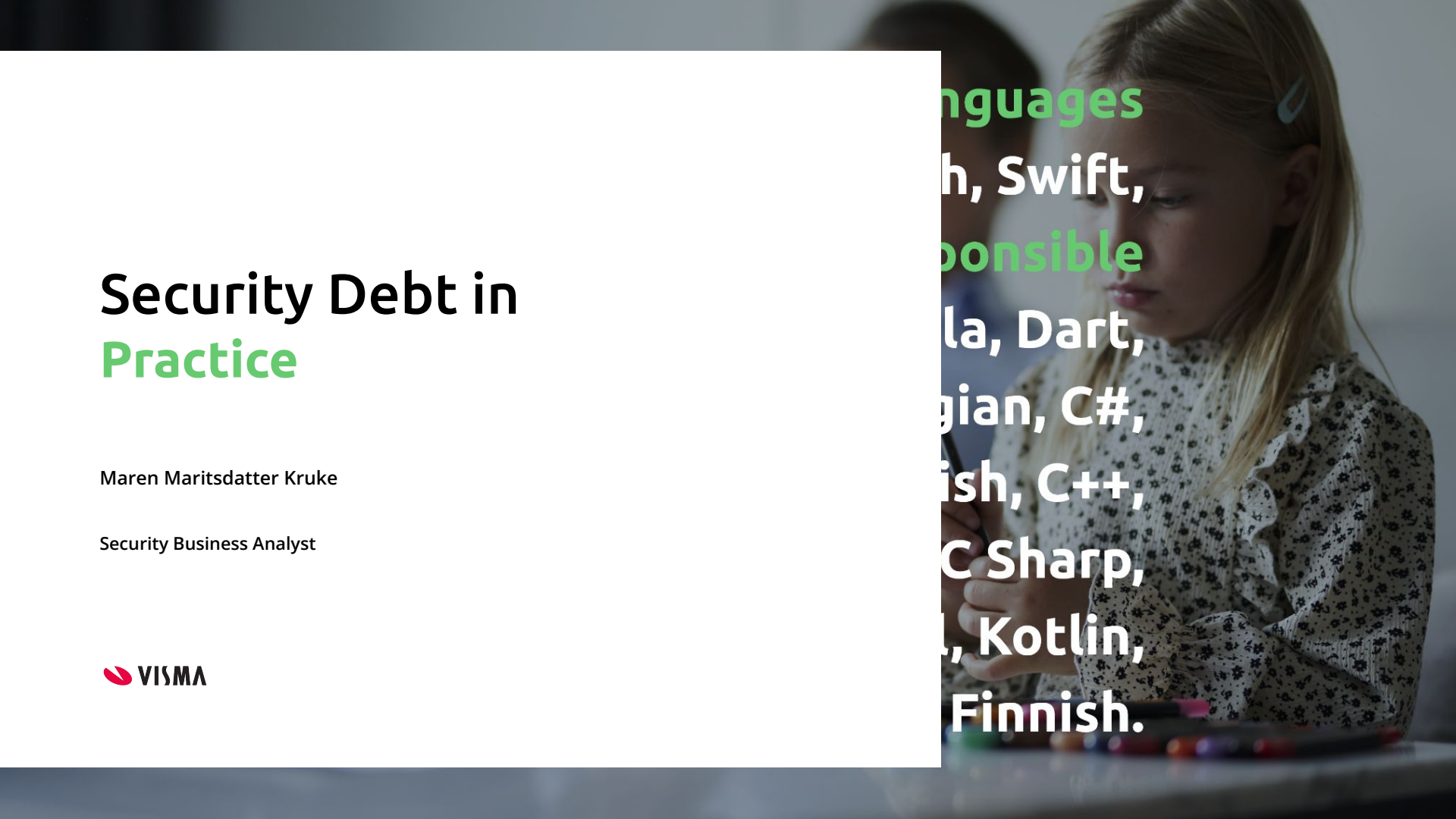
Security Debt in Practice

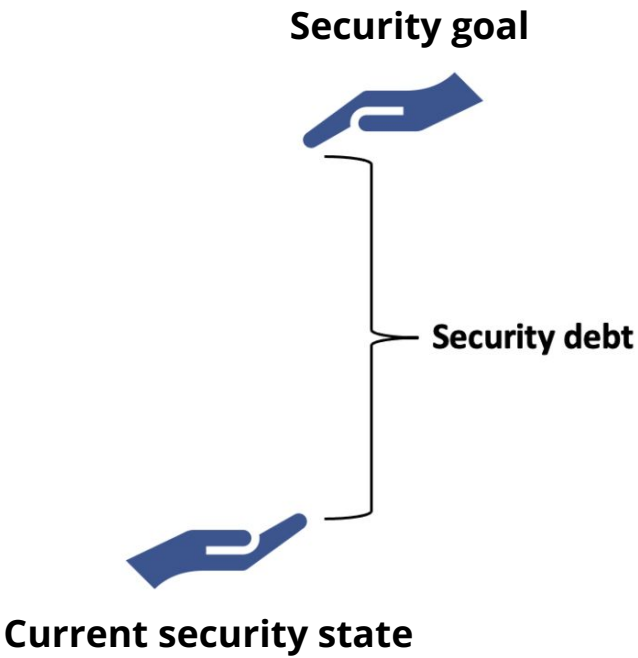
Maren Maritsdatter Kruke

Security Business Analyst

VISMA



Security goal



"It is clearly an evolution, so you are between two levels of security and you are on the wrong one, the lower one, so if you are there, you are not allowed to stay there because it's a danger and a risk."

"I'm thinking that we have some sort of quality criteria or imagination of how the system should be, good quality or really secure. So we have our vision here ["*right hand raised high*"] and we have our state over here ["*left hand underneath right hand*"] and over here ["*the section between the two hand placements*"] is the debt."

VISMA

Security debt definition

“Security debt is a set of design or implementation solutions that hinder or has the potential to hinder the achievement of a system’s security goal”

VISMA

Technical debt definition

“In software-intensive systems, technical debt is a collection of design or implementation constructs that are expedient in the short term, but set up a technical context that can make future changes more costly or impossible. Technical debt presents an actual or contingent liability whose impact is limited to internal system qualities, primarily maintainability and evolvability.”

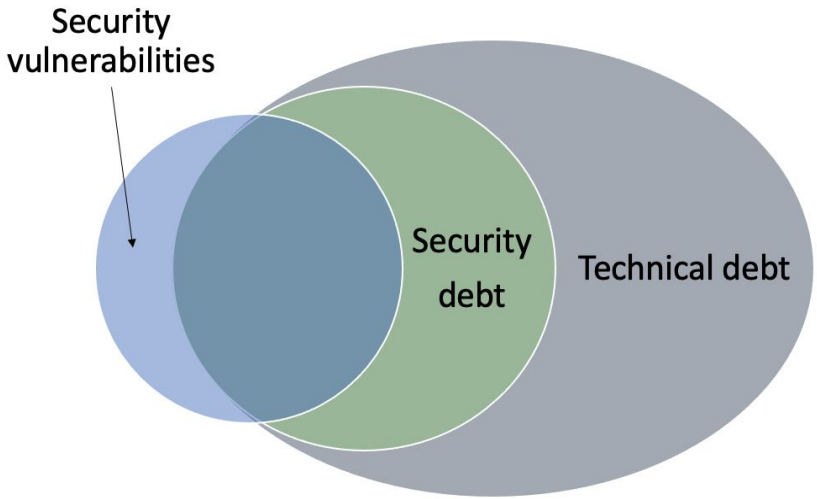
(Dagstuhl Seminar 16162, https://drops.dagstuhl.de/opus/volltexte/2016/6693/pdf/dagrep_v006_i004_p110_s16162.pdf)

Security debt definition

“Security debt is a set of design or implementation solutions that hinder or has the potential to hinder the achievement of a system’s security goal”

VISMA

Security debt, security vulnerabilities, and technical debt relationship



VISMA

Security debt management

- Identification
  - Bug Bounty
  - Security testing performed by a security team in Visma
- Prevention
  - Threat modelling
- Documentation
- Analysis
- Planning
- Repayment

Monitoring

Communication

VISMA

Security Debt in Practice

Maren Maritsdatter Kruke

Security Business Analyst

VISMA