Measuring software security

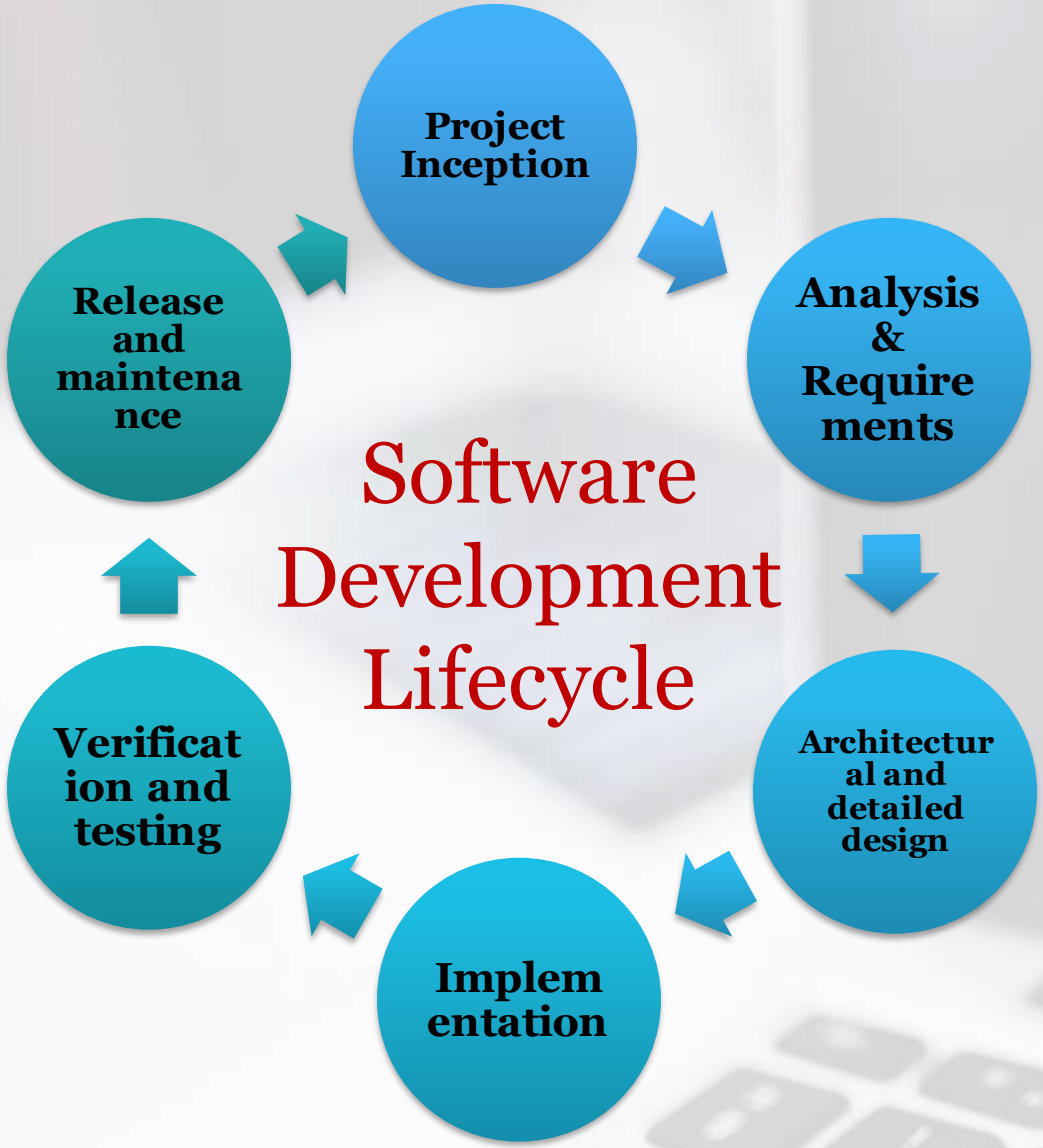
Arina Kudriavtseva

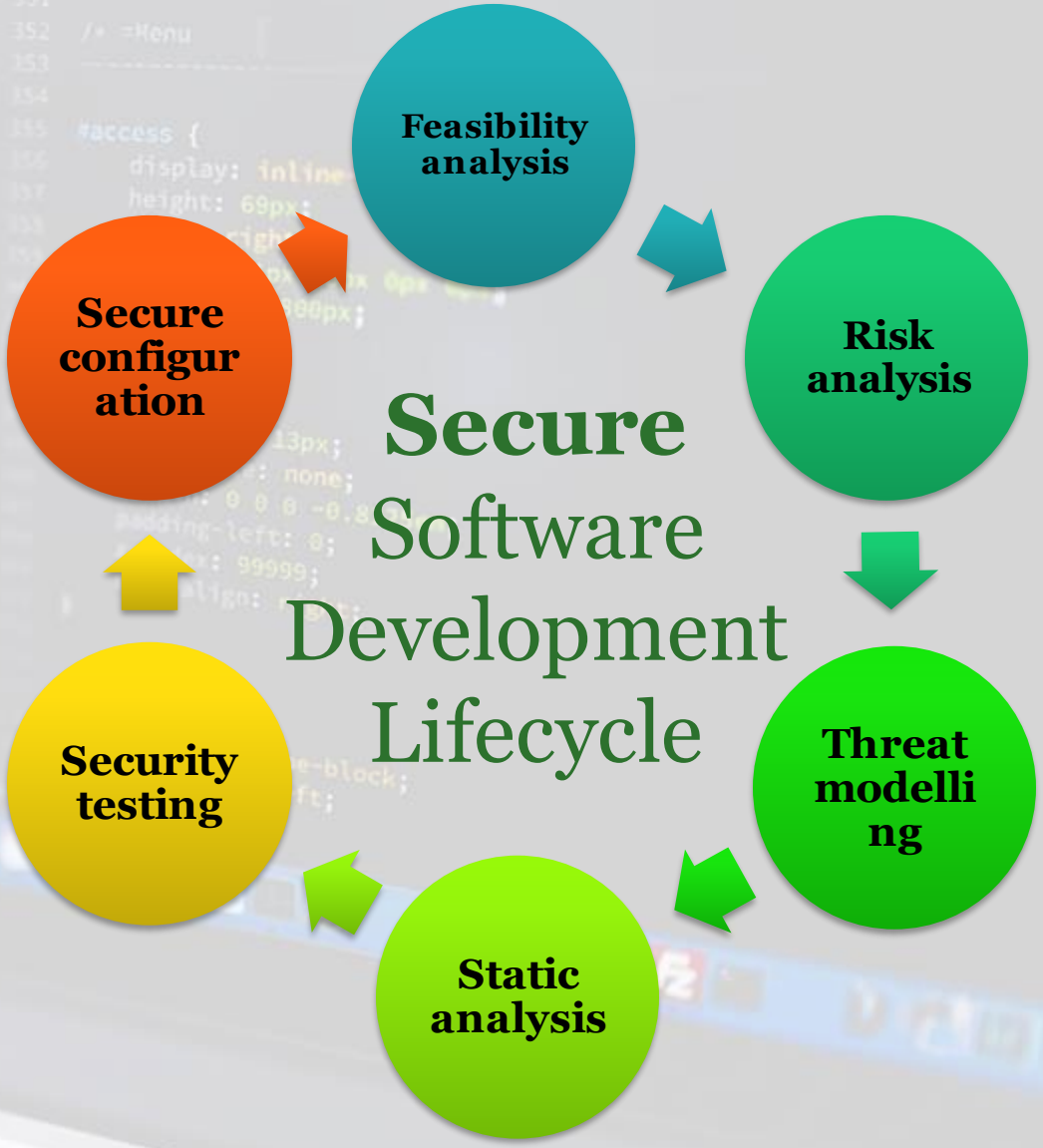
Universiteit Leiden
The Netherlands

C-SIDE Project

The goal of the project is to propose a methodology for software development that will improve software security.

What is methodology?





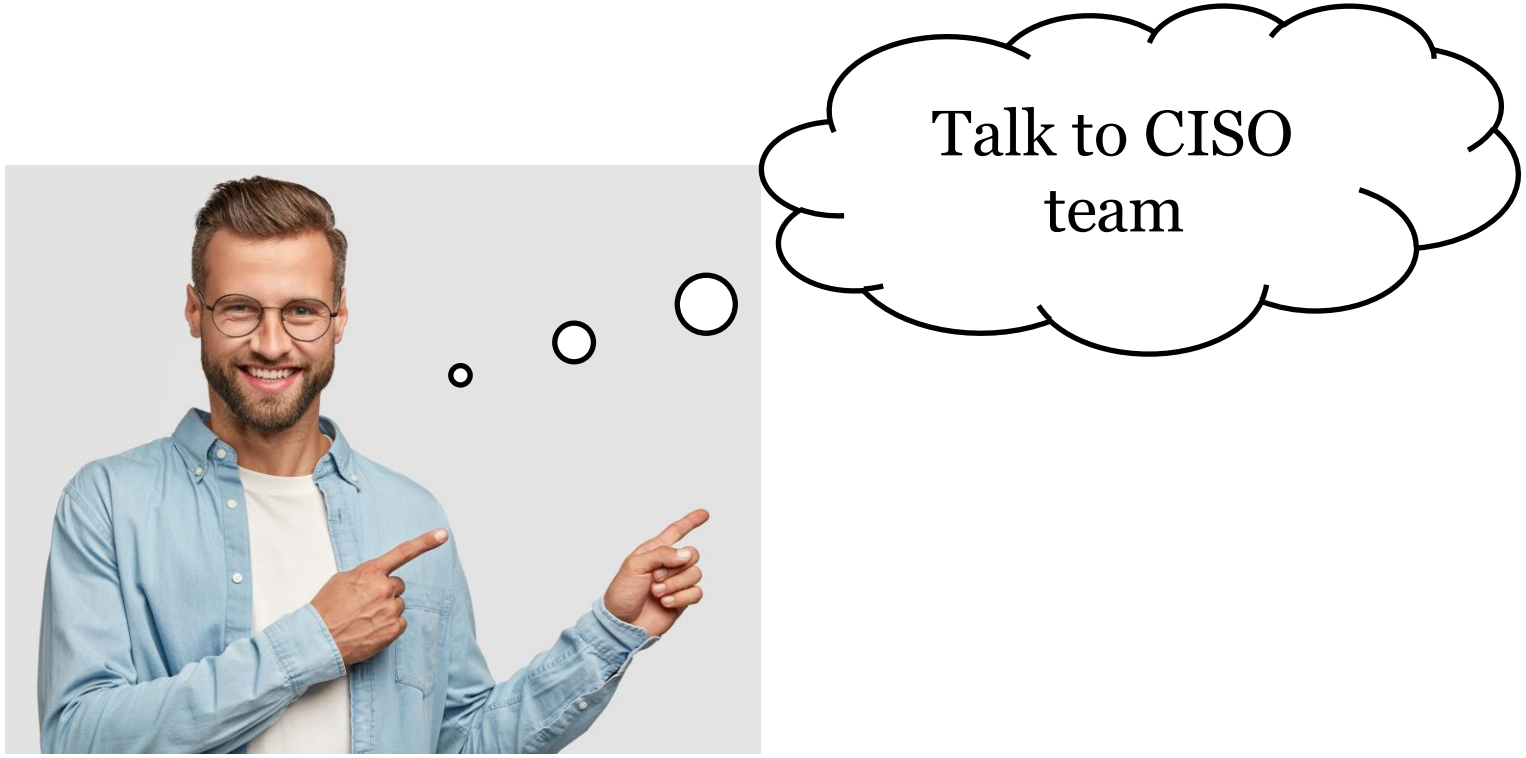
The research questions

- How security is assessed quantitatively?
- How security is assessed qualitatively?
- What is the decision making process what security analyst follows based on the collected security metrics and qualitative indicators?

Who really makes the decisions?

The development team

Who really makes the decisions?



Who really makes the decisions?

CISO team

Who really makes the decisions?

Can security be represented as 1 number?

8 of 10: absolutely not. Security is too complex

1 out of 10: it’s possible, we are working on it

1 out of 10: security is always binary

How secure is your software today?

8 out of 10 : we care about security more than our competitors, security practices, compliance

1 out of 10: we are secure

1 out of 10: “The S in IoT stands for security”

Are we shifting measurements left?

10 out of 10 :

NO. It’s not interesting

2 out of 10:

Security-by-design is impossible

What do you measure but ignore?

2 out of 10:

We ignore everything

8 out of 10:

- Vulnerabilities in dependencies
- Mediums and lows
- Metrics related to technologies, people, processes

What would you like to measure?

- Unknown vulnerabilities
- Usage patterns by users
- Code compliance with architectural guidance
- Security awareness and knowledge
- Completeness of the threat model
- Threats that are coming

Is security about vulnerabilities?

2 out of 10 : NO

1 out of 10 : Yes: vulnerabilities found in pentest

3 out of 10: Depends on how it's tested

2 out of 10: YES

2 out of 10: Only critical vulnerabilities

Problems we have

- We don’t measure vulnerabilities
- Too many false positives
- Testing tools are expensive
- Measure old threats
- Communicate the metrics to the board

Thank you!

Universiteit
Leiden
The Netherlands

Discover the world at Leiden University