Using Secure Software Engineering Metrics to support the automated calculation and visualization of Team Security Maturity in Agile Development Projects

Timo Zandonella, Master‘s Thesis

19.12.2022, Advanced Seminar

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Motivation: Monitoring the security level during the development process

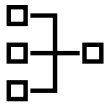
Addressing security in software engineering becomes increasingly important [1], but it can often be challenging to measure the security level in a team or a product [2]

With **team security maturity** it is possible to capture the capabilities of an agile development team to develop secure and security-compliant software [1]

The maturity provides insight for different stakeholders at different organizational levels [3, 4, 5]

Focus areas for security

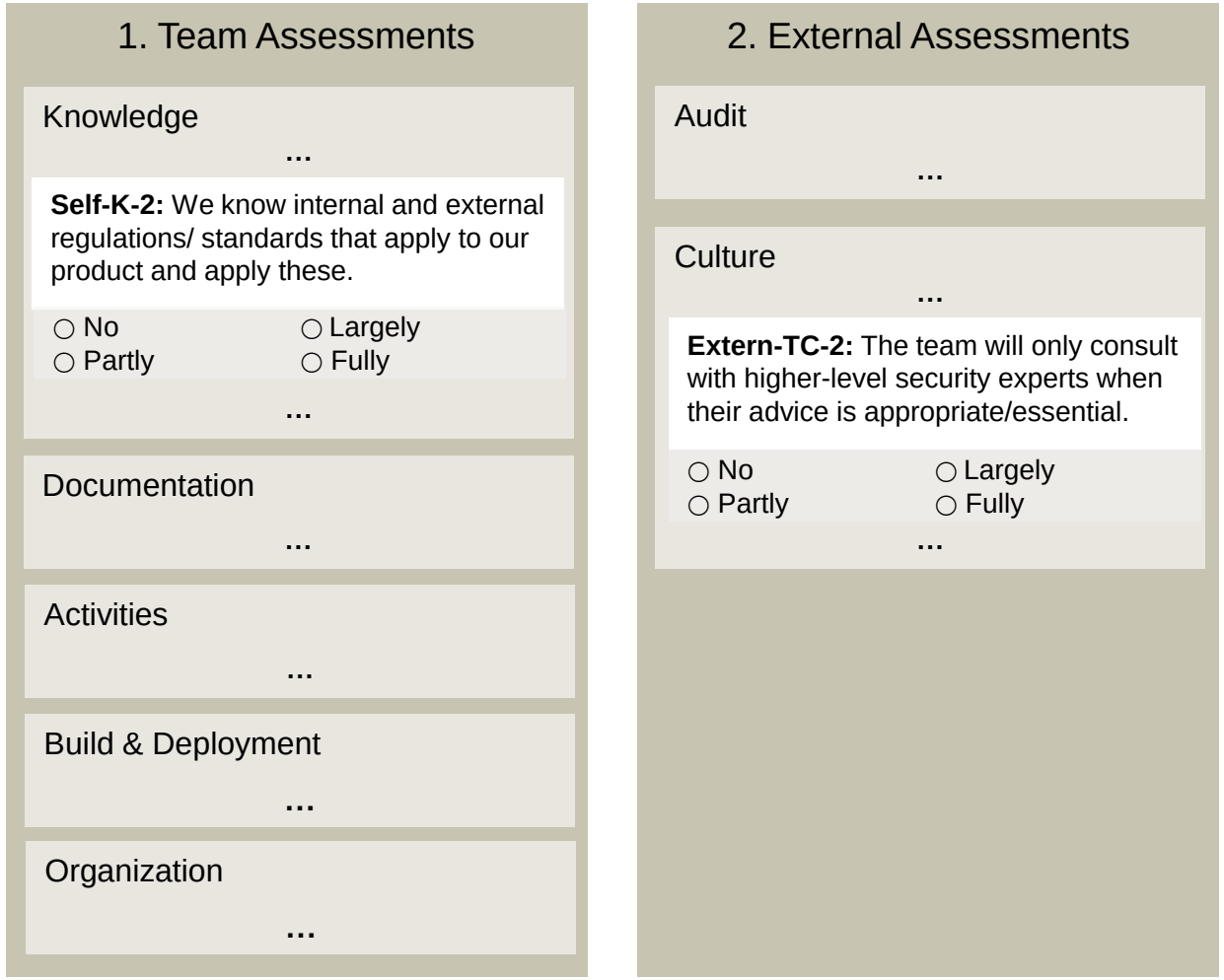
Team autonomy



Organizational security overview

Motivation: Monitoring the security level during the development process

Within the Team Security Maturity Model (TSMM), the information is captured for various domains [6]



Goal: Improve the maturity calculation with security metrics

However, assessments are used for the information collection, which can have some limitations [7, 8]

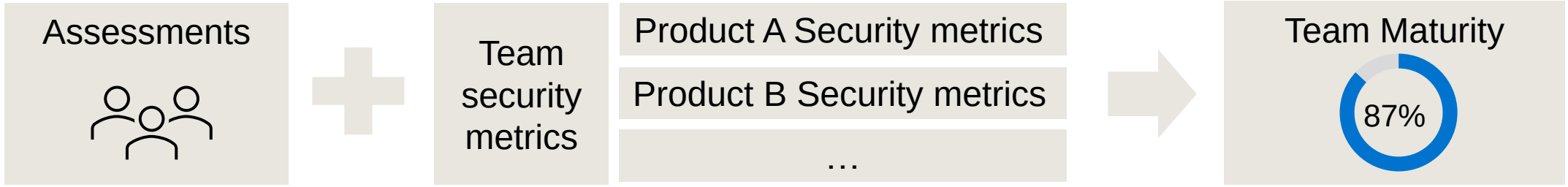
- Time-consuming to carry out
- Potential subjectivity
- Periodic instead of continuous analysis

To address these problems, we introduce security metrics measuring the team's capabilities and product imperfections

e.g. Security Regulation Review Rate | Unsecured Endpoints Rate

Goal of the thesis:

Improve the team security maturity calculation with security metrics



Outline

Research Questions and Artifacts

RQ1: Which security metrics exist and how can they automatically be captured with the support of security tools?

- Methodology: Systematic Literature Review
- Objective: Catalogue of Security Metrics

RQ2: How can security metrics be used to assess the security maturity of an agile development team?

- Objective: Integration into TSMM
- Objective: Maturity Calculation

RQ3: How can a team‘s security maturity be calculated, represented and visualized in a self-assessment tool?

- Objective: Demo of Prototype
- Methodology: Evaluation

Summary

Outlook

Research Questions and Artifacts

Research Questions and Methodology

RQ1: Which security metrics exist and how can they be automatically be capture with the support of security tools?

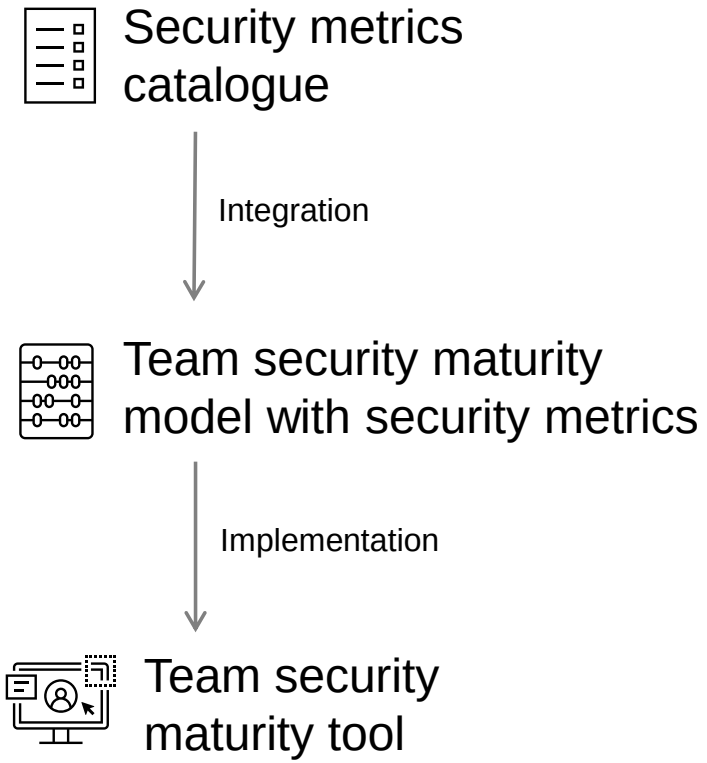
Methodology: Systematic literature review,
Structured metrics qualification procedure

RQ2: How can security metrics be used to assess the security maturity of an agile development team?

RQ3: How can a team‘s security maturity be calculated, represented and visualized in a self-assessment tool?

Methodology: Evaluation with expert interviews

Artifacts



Outline

Research Questions and Artifacts

RQ1: Which security metrics exist and how can they automatically be captured with the support of security tools?

- Methodology: Systematic Literature Review
- Objective: Catalogue of Security Metrics

RQ2: How can security metrics be used to assess the security maturity of an agile development team?

- Objective: Integration into TSMM
- Objective: Maturity Calculation

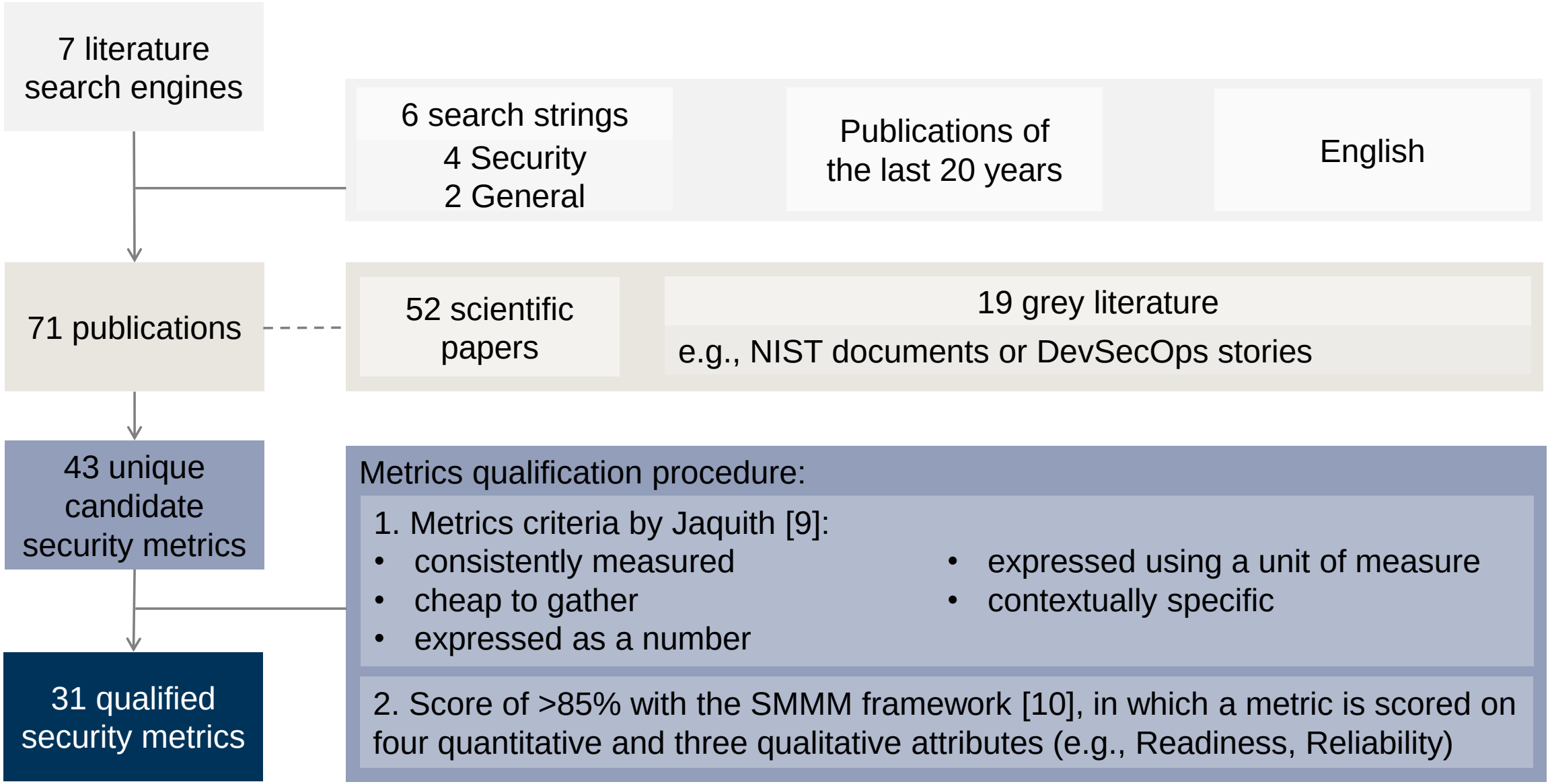
RQ3: How can a team‘s security maturity be calculated, represented and visualized in a self-assessment tool?

- Objective: Demo of Prototype
- Methodology: Evaluation

Summary

Outlook

Methodology: Systematic Literature Review



A metric is described in a structured way

The metric description follows a catalogue format proposed by Bouwers et al. [11]

Qualitative Fields		Quantitative Fields	
Name	Company Security Policy Review Rate (CSPRR)	**Level**	derived
Entity	Company security policies	**Type**	internal
Attribute	Review rate	**Range**	[0,100]
Definition	Security policies reviewed / Amount of security policies	**Expected Value**	100
Rationale (theoretical)		**Variability**	[-10,10]
Percentage of relevant company security policies reviewed		**Scale Type**	ratio
Implications (practical)		**Related metrics**	
Company security policy awareness is often low and increasing it can lead to more informed decision in early SDLC phases (shifts security left).		Government Security Regulation Review Rate (GSRRR)	
Applicable in context		**Validation**	
Large enterprise with a central security unit		[12,13,14,15]	
Solution Strategies			
Company security policy workshops, allow time for review			

A metric is described in a structured way

Two additional fields describe the level of automation of the metric

Automation	~~○ Manual~~ ~~◐ Semi automated~~ ● Automated
Tool Category	◯ ~~Static application security testing (SAST)~~ ◯ ~~Dynamic application security testing (DAST)~~ ◯ ~~Interactive application security testing (IAST)~~ ◯ ~~Software composition analysis (SCA)~~ ◯ ~~Vulnerability management tool (VMT)~~ ◯ ~~Security information and event management (SIEM)~~ ⊗ Project management tool (PMT)

A collection of security metrics in a structured security metrics catalogue

The catalogue is split into metrics measuring team-wide capabilities and product-specific activities; in addition, metrics are categorized into different domains

Team security metrics	
Knowledge	Effort
2 metrics	4 metrics

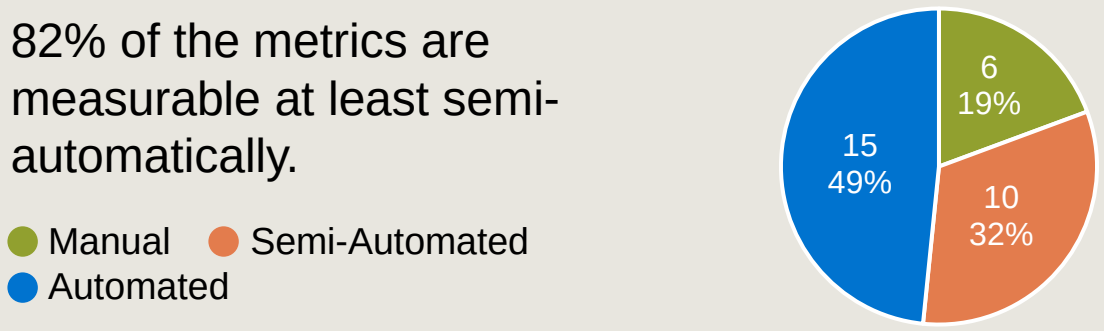
Product security metrics				
Analysis	Design	Implementation	Deployment	Maintenance
3 metrics	5 metrics	6 metrics	8 metrics	3 metrics

Name	Rationale
Architecture Component Attack Surface Analysis Rate	Percentage of proposed architecture components subject to attack-surface analysis
Architecture Component Architectural Risk Analysis Rate	Percentage of proposed architecture components subject to architectural risk analysis
Security Requirements Satisfying Architecture Components Rate	Percentage of software components with demonstrated satisfaction of security requirements specifications
…	

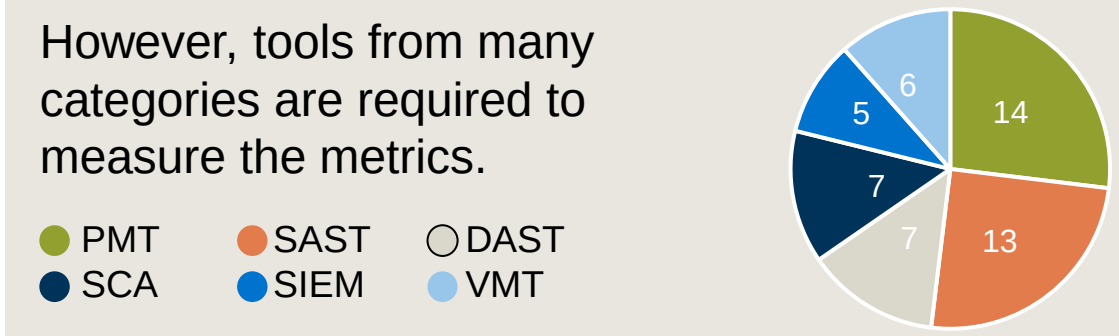
The catalogue reveals insights into the nature of security metrics

The level of automation varies between the metrics

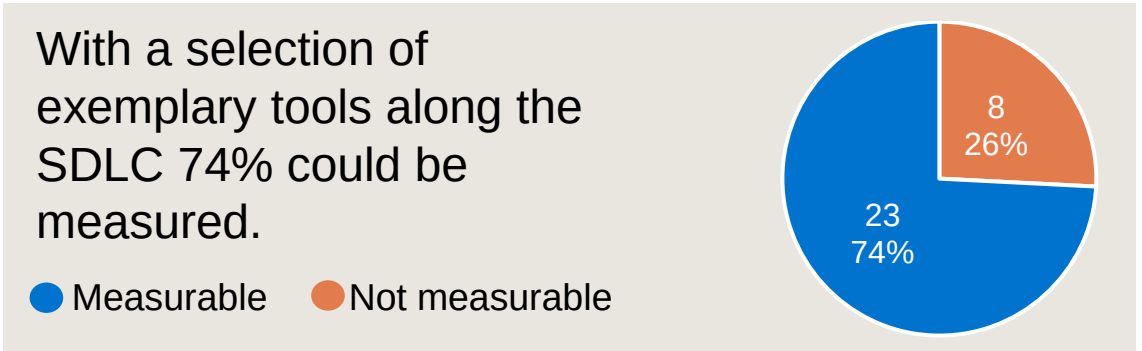
82% of the metrics are measurable at least semi-automatically.



However, tools from many categories are required to measure the metrics.



With a selection of exemplary tools along the SDLC 74% could be measured.



Outline

Research Questions and Artifacts

RQ1: Which security metrics exist and how can they automatically be captured with the support of security tools?

- Methodology: Systematic Literature Review
- Objective: Catalogue of Security Metrics

RQ2: How can security metrics be used to assess the security maturity of an agile development team?

- Objective: Integration into TSMM
- Objective: Maturity Calculation

RQ3: How can a team‘s security maturity be calculated, represented and visualized in a self-assessment tool?

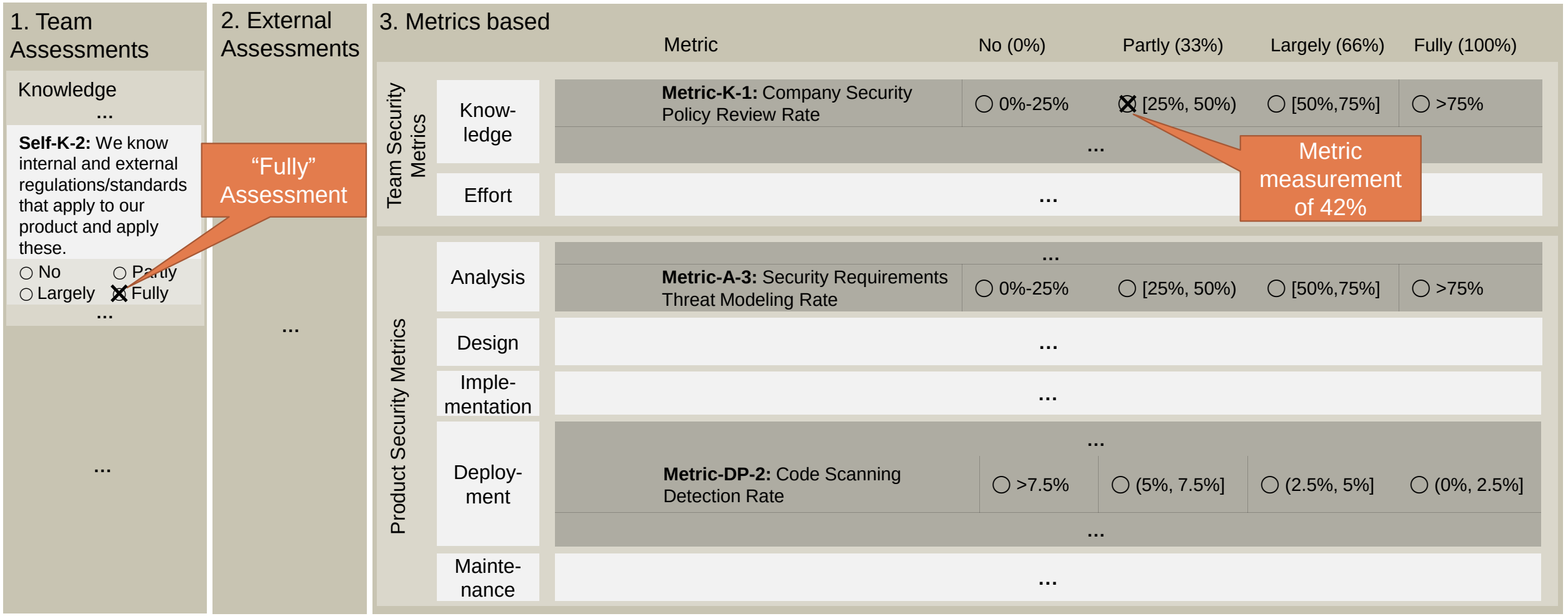
- Objective: Demo of Prototype
- Methodology: Evaluation

Summary

Outlook

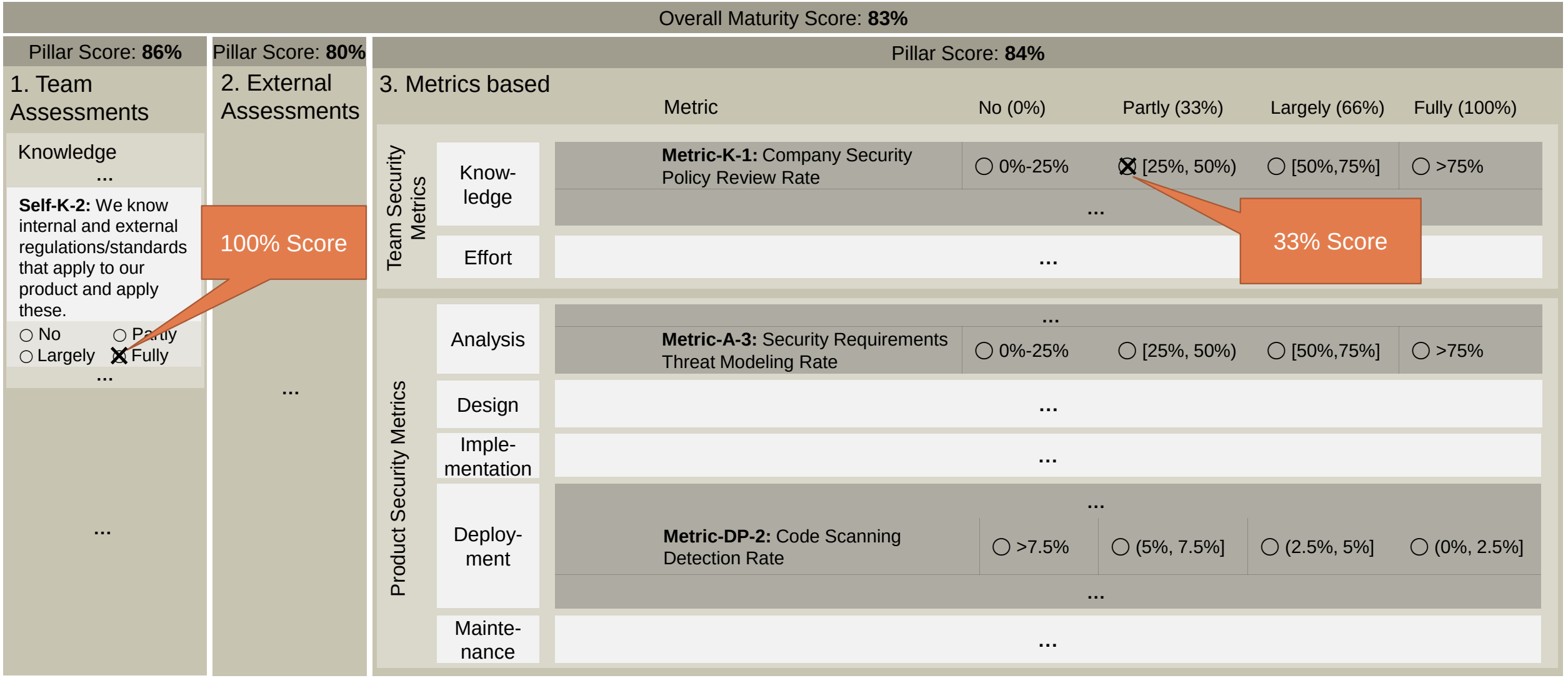
The collected metrics can be integrated into the team security maturity model

The metrics are integrated into a third TSMM pillar named “metrics based” in addition to the existing assessments



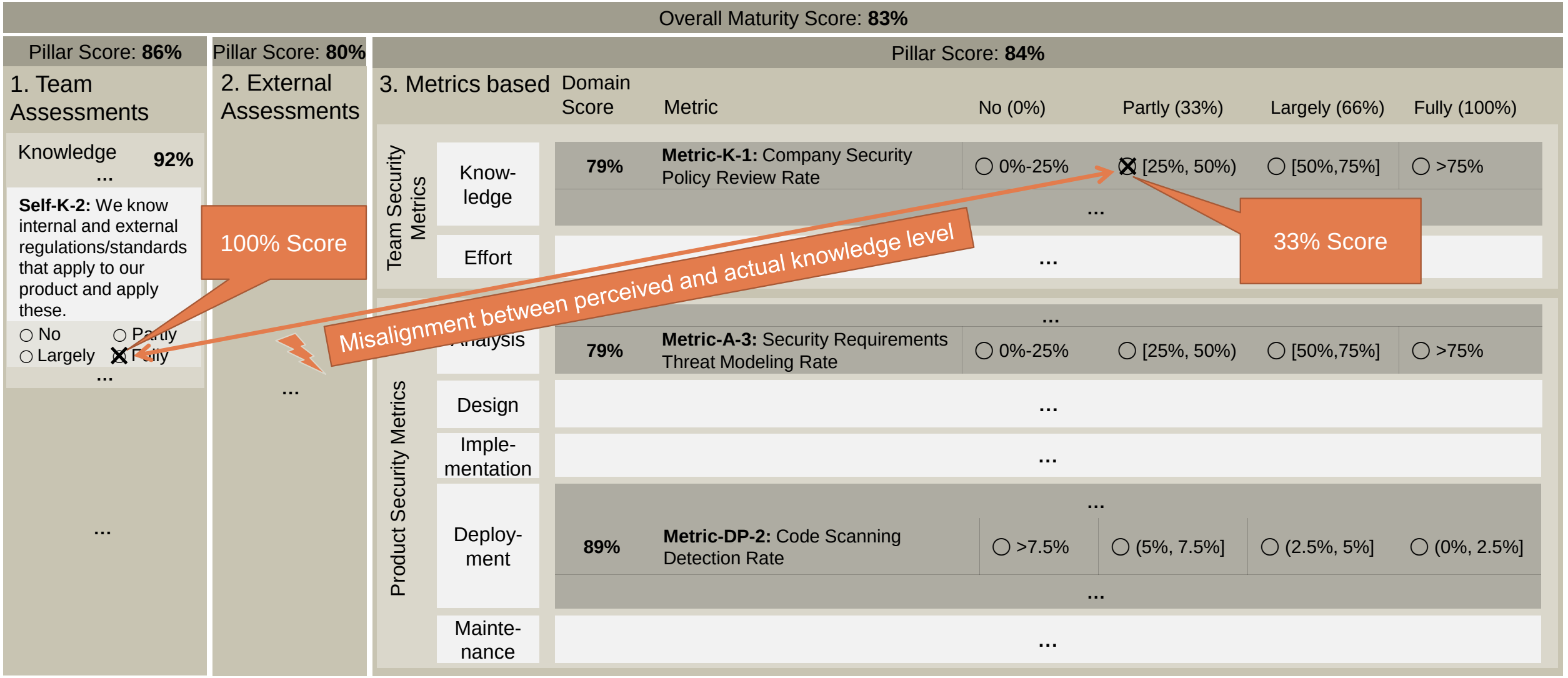
From the collected maturity information an overall score can be calculated

First the scores of the assessments and measurements are aggregated into their domains and pillars; finally, the overall maturity score can be calculated



Additional types of insight can be gained from the maturity model

The assessments can be supported or refuted by the metric measurements



Outline

Research Questions and Artifacts

RQ1: Which security metrics exist and how can they automatically be captured with the support of security tools?

- Methodology: Systematic Literature Review
- Objective: Catalogue of Security Metrics

RQ2: How can security metrics be used to assess the security maturity of an agile development team?

- Objective: Integration into TSMM
- Objective: Maturity Calculation

RQ3: How can a team‘s security maturity be calculated, represented and visualized in a self-assessment tool?

- Objective: Demo of Prototype
- Methodology: Evaluation

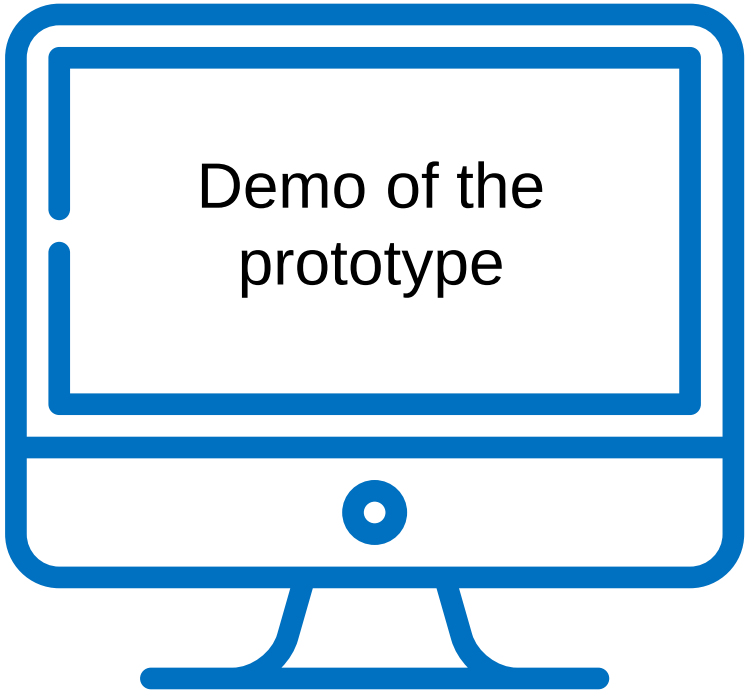
Summary

Outlook

The developed prototype collects TSMM information and displays it

To enable the automatic calculation, a team security maturity tool was developed, which can collect metric measurements from external security tools and calculate the maturity score

Afterwards an evaluation about the approach and the prototype was conducted with eight experts



Evaluation with expert interviews

To evaluate the approach and the prototype, we carried out semi structured interviews with eight experts according to the ACM standard for qualitative surveys

Team security maturity approach

›	Security efforts and measuring during development were reported as insufficient
+	For guidance during development, security maturity was regarded as innovative and useful
+	Security metrics are a beneficial extension, as assessments generally were considered tedious
?	Context influences the required security levels, which a security model needs to consider
?	Teams should only benefit from the maturity calculation, never get punished

Tool support with the prototype

›	To use the model a security maturity dashboard and automatic metric measurement is required
+	The prototype includes verbose information about all parts of the model within a clear structure
+	Solution strategies help address the security issues and should be the focus of the tool
?	Model or organization reference scores are required to interpret the maturity score
?	The success depends on the capability to collect measurements from external security tools

Outline

Research Questions and Artifacts

RQ1: Which security metrics exist and how can they automatically be captured with the support of security tools?

- Methodology: Systematic Literature Review
- Objective: Catalogue of Security Metrics

RQ2: How can security metrics be used to assess the security maturity of an agile development team?

- Objective: Integration into TSMM
- Objective: Maturity Calculation

RQ3: How can a team‘s security maturity be calculated, represented and visualized in a self-assessment tool?

- Objective: Demo of Prototype
- Methodology: Evaluation

Summary

Outlook

Summary

- The security metrics catalogue contains insightful metrics in a structured format
- Most security metrics can be automated, but currently measurement requires effort
- By integrating security metrics into team security maturity, the calculation and insights are enhanced
- Tool-supported maturity can help teams develop secure software

Outlook

In the future, research could be conducted using the artifacts as a foundation

Investigating if the maturity approach could be used for other non-functional requirements
For instance, usability, maintainability, or performance can be measured with metrics

Validating the security maturity approach and tool in organizations
Industry case study to study the security capabilities of a team using the maturity tool over time or to a control group

Thank you for your attention!

Q & A

Sources

[1] CSIS. Significant Cyber Incidents Since 2006. Tech. rep. Center for Strategy & International Studies, 2022.

[2] Rindell, Kalle & Ruohonen, Jukka & Holvitie, Johannes & Hyrynsalmi, Sami & Leppänen, Ville. (2020). Security in agile software development: A practitioner survey. Information and Software Technology. 131. 106488.
DOI: 10.1016/j.infsof.2020.106488.

[3] U. Kulkarni and R. St Louis. “Organizational Self Assessment of Knowledge Management Maturity”. In: 2003, p. 332.

[4] C. Steinmann and H. Stienen. “SynQuest - Tool Support for Software Self-Assessments”. In: Software Process: Improvement and Practice 2.1 (1996), pp. 5–12. ISSN: 1077-4866.
DOI: 10.1002/(SICI)1099-1670(199603)2:1<5::AID-SPIP33>3.0.CO;2-U.

[5] Schenk, Nathalie, An Adaptive Approach for Security Compliance in Large-Scale Agile Software Development. 2022. Technical University Munich.

[6] Watzelt, J.-P. (2022). Design and Implementation of a Team Maturity Model Assessing Security Compliance in Large-Scale Agile Software Development. Technical University Munich.

[7] R. Pemberton, ed. Taking control. Autonomy in language learning. Hong Kong: Hong Kong University Press, 2010. 337 pp. ISBN: 9789882202856.

[8] A. Poth, M. Kottke, T. Mahr, and A. Riel. “Teamwork quality in technology-driven product teams in large-scale agile organizations”. In: Journal of Software: Evolution and Process (2021), e2388. ISSN: 2047-7473.
DOI: 10.1002/smr.2388.

[9] A. Jaquith. Security Metrics. Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional, 2007, p. 336. ISBN: 9780321349989.

[10] S. M. Muthukrishnan and S. Palaniappan. “Security metrics maturity model for operational security.” In: 2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE, May 2016. DOI: 10.1109/iscaie.2016.7575045.

[11] E. Bouwers, A. v. Deursen, and J. Visser. “Towards a Catalog Format for Software Metrics.” In: Proceedings of the 5th International Workshop on Emerging Trends in Software Metrics. WETSoM 2014. Hyderabad, India: Association for Computing Machinery,2014, pp. 4447. ISBN: 9781450328548. DOI: 10.1145/2593868.2593876.

[12] W. K. Brotby and G. Hinson. PRAGMATIC Security Metrics. Taylor & Francis Ltd., Apr. 2016. 512 pp. ISBN: 1439881537.

[13] M. Rudolph and R. Schwarz. “A Critical Survey of Security Indicator Approaches.” In: 2012 Seventh International Conference on Availability, Reliability and Security. IEEE, Aug. 2012. DOI: 10.1109/ares.2012.10.

[14] E. Kahraman. Evaluating IT security performance with quantifiable metrics. July 2008.

[15] S. M. Poremba. CIS to release consensus IT security metrics. https://www.scmagazine.com/news/breach/cis-to-release-consensus-it-security-metrics. 2008.