Towards Automated Continuous Security Compliance

Vision Paper

24.10.2024 | Florian Angermeir[1,2]

Jannik Fischbach[1,3]
Fabiola Moyón[4,5]
Daniel Mendez[2,1]

1 fortiss
2 Blekinge Institute of Technology
3 Netlight Consulting GmbH
4 Siemens Technology
5 Technical University of Munich

Agenda

Background

Security Compliance
&
Continuous Software Engineering

Contributions

Continuous Security Compliance

Challenges in Continuous Security Compliance

Research Design

What happened so far?

What is currently in progress?

What are the next steps?

Background

Background

What is the problem?

Continuous Software Engineering

- Fast paced customer value delivery
- Continuous improvement
- Continuous experimentation

Security Compliance

- Manual activities (Requirements extraction, .., compliance assessment)
- Rigid processes
- Extensive documentation

Summary

- Traditional compliance activities incompatible with continuous software engineering principles
- Issue for companies in highly regulated domains

Background

Research Goals

Research Goals

RG1) Challenges of security compliance in continuous software engineering
RG2) Requirements and constraints for automation
RG3) Potential and limitations for automation as treatment
RG4) Develop and evaluate treatments

Contributions

Contributions

What is *"Continuous Security Compliance"*?

Scanned literature for CSC definitions

"Combining CC [Continuous Compliance] and CS [Continuous Security] through the holistic view of standardisation that spans across people, processes, and technology. Regulatory requirements are utilised to derive security activities and integrate security into a process while making it standards-compliant" [1]

Scanned literature for Continuous Compliance definitions

12 relevant resources [4-13]
Solution independent definitions in [2,3]

Extracted relevant concepts

1. Continuous execution of compliance activities
2. Adherence to regulatory requirements
3. Compliance over entire development life-cycle
4. (New) Continuous Software Engineering background

Contributions

What is *“Continuous Security Compliance“*?

Continuous Security Compliance (CSC) is a set of practices…

- to ensure product and process adherence
- to requirements derived from relevant security regulatory sources,
- integrated holistically into the product development life-cycle,
- following continuous software engineering principles and goals.

Contributions

Challenges in Continuous Security Compliance

Past

Performed workshops with three companies (see [14]): Security compliance in continuous software engineering
15 challenges in Continuous Security Compliance, 4 general solutions streams

[14] Fabiola Moyón, Florian Angermeir, and Daniel Mendez. 2024. Industrial Challenges in Secure Continuous Development. In ICSE ’24. 3 pages.

Contributions

Challenges in Continuous Security Compliance

Past

Performed workshops with three companies (see [14]): Security compliance in continuous software engineering
15 challenges in Continuous Security Compliance, 4 general solutions streams

Our Contribution

Performed literature review to validate/extend challenges of [14]
Validated 9 challenges, extended 12 challenges

[14] Fabiola Moyón, Florian Angermeir, and Daniel Mendez. 2024. Industrial Challenges in Secure Continuous Development. In ICSE ’24. 3 pages.

Contributions

Challenges in Continuous Security Compliance

Past

Performed workshops with three companies (see [14]): Security compliance in continuous software engineering
15 challenges in Continuous Security Compliance, 4 general solutions streams

Our Contribution

Performed literature review to validate/extend challenges of [14]
Validated 9 challenges, extended 12 challenges

Why Automation?

In [14] practitioners identified automation as solution to treat some of the challenges. E.g.

- *„Get security activities into early feedback principle of DevOps“*

In this paper we found further such challenges. E.g.

- *„Security compliance evidence generation and documentation is too time consuming“*

[14] Fabiola Moyón, Florian Angermeir, and Daniel Mendez. 2024. Industrial Challenges in Secure Continuous Development. In ICSE ’24. 3 pages.

Contributions

Challenges in Continuous Security Compliance

Past

Performed workshops with three companies (see [14]): Security compliance in continuous software engineering
15 challenges in Continuous Security Compliance, 4 general solutions streams

Our Contribution

Performed literature review to validate/extend challenges of [14]
Validated 9 challenges, extended 12 challenges

Why Automation?

In [14] practitioners identified automation as solution to treat some of the challenges. E.g.

- *„Get security activities into early feedback loops“*
- *„Match security compliance requirements with working pipelines“*

In this paper we found further such challenges. E.g.

- *„Changes to requirement, design or implementation break system security requirements“*
- *„Security compliance evidence generation and documentation is too time consuming“*

Automation alone won’t solve everything

BUT it is likely to be a significant factor in addressing many challenges in CSC

Research Design

Research Design

Background

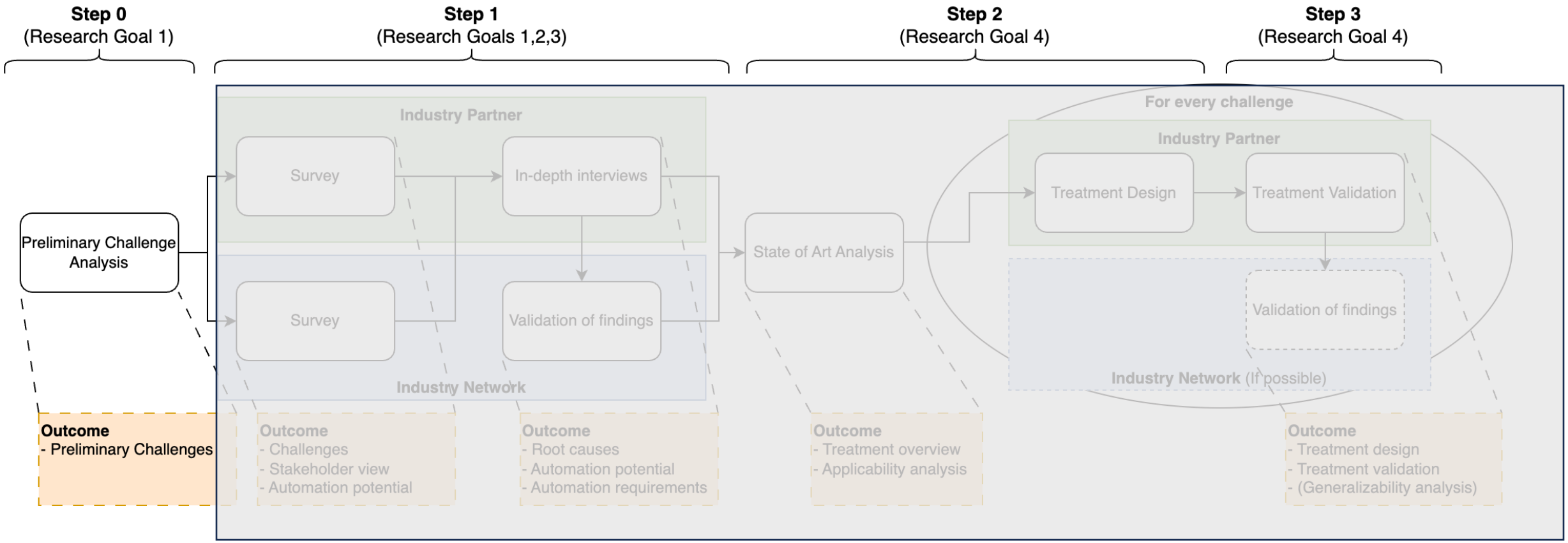
Research Goals

RG1) Challenges of security compliance in continuous software engineering
RG2) Requirements and constraints for automation
RG3) Potential and limitations for automation as treatment
RG4) Develop and evaluate treatments

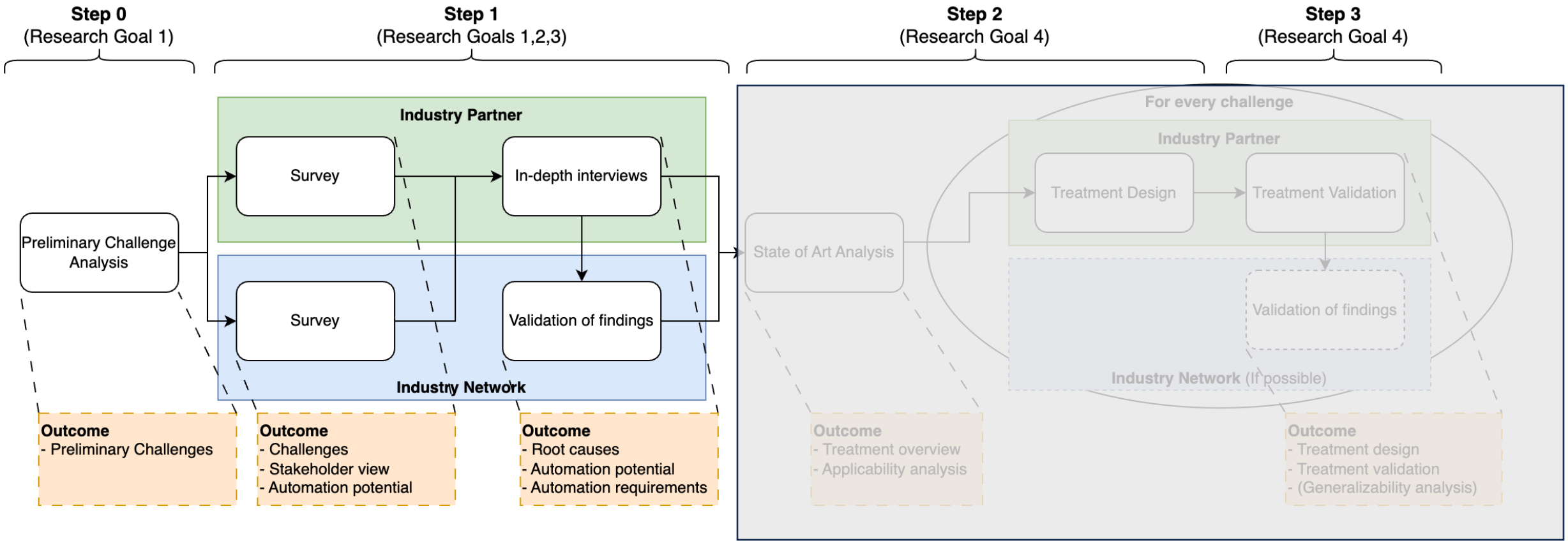
Research Environment

Industrial partner: Large enterprise in highly regulated domains, research in last 5 years in security compliance
Large-scale academia-industry network: Various companies and research streams

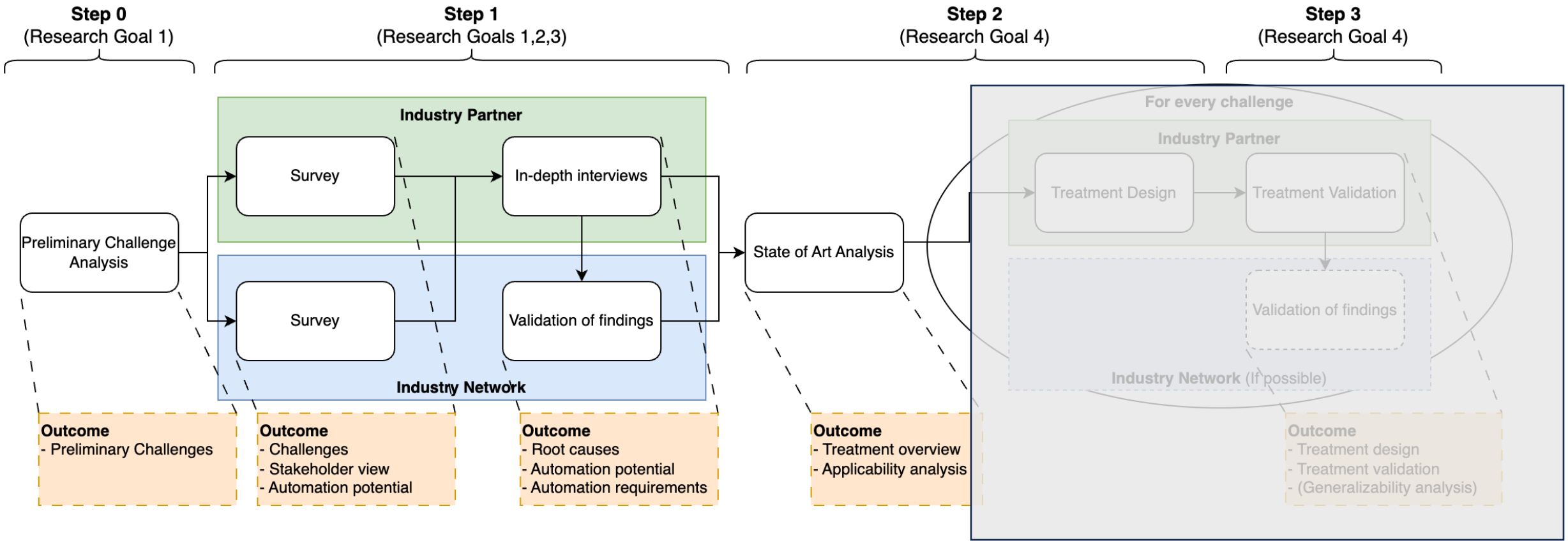
Research Design



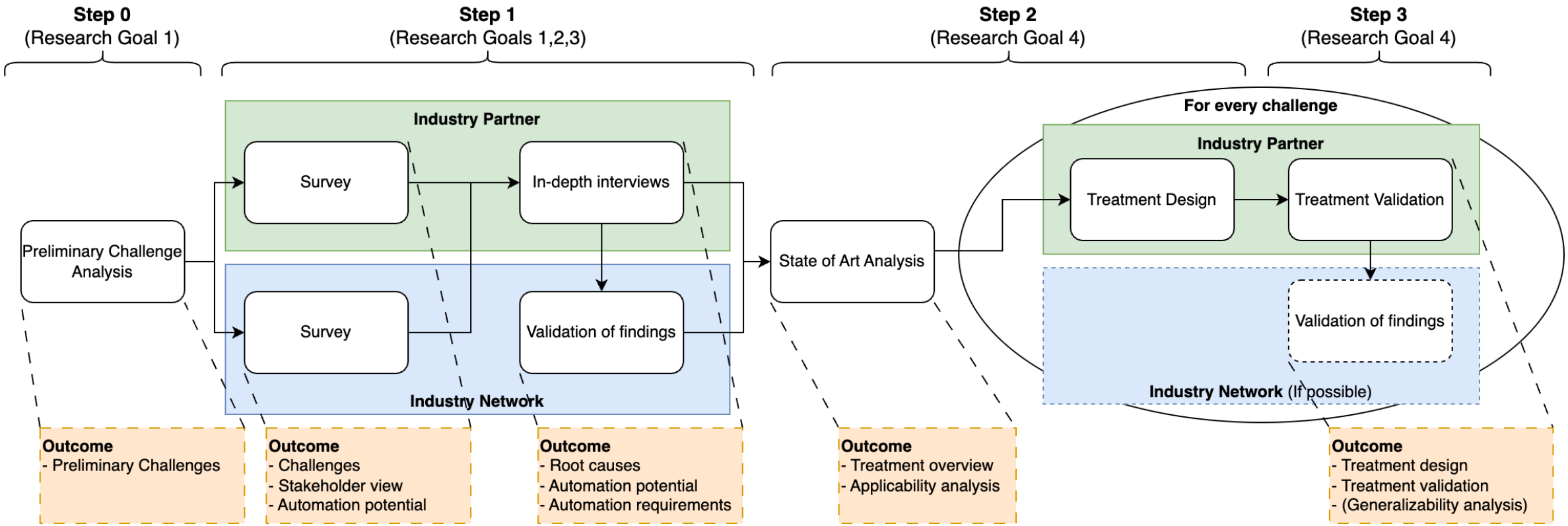
Research Design



Research Design



Research Design



Questions & Feedback

Key Takeaway 1

Continuous Security Compliance is a set of practices to ensure product and process adherence to requirements derived from relevant security regulatory sources, integrated holistically into the product development life-cycle, following continuous software engineering principles and goals.

Key Takeaway 2

We validated 9 of the challenges of [14] in literature and extracted 12 further challenges. Total of 27 challenges.

Key Takeaway 3

Automation will likely play a key role in enabling continuous security compliance.

References

[1] Fabiola Moyón, Daniel Méndez, Kristian Beckers, and Sebastian Klepper. 2020. How to Integrate Security Compliance Requirements with Agile Software Engineering at Scale? In PROFES '20. 69–87.
[2] Brian Fitzgerald and Klaas-Jan Stol. 2014. Continuous Software Engineering and beyond: Trends and Challenges. In RCoSE '14. 1–9.
[3] Tiziano Santilli, Patrizio Pelliccione, Rebekka Wohlrab, and Ali Shahrokni. 2023. What is Continuous Compliance? IEEE Software (12 2023), 1–10.
[4] Muhammad Zaid Abrahams and Josef J Langerman. 2018. Compliance at Velocity within a DevOps Environment. In ICDIM '18. 94–101.
[5] Suresh Chari, Ian Molloy, Youngja Park, and Wilfried Teiken. Ensuring continuous compliance through reconciling policy with usage. In SACMAT '13. 49-60.
[6] IBM. 2013. Maintaining continuous compliance—a new best-practice approach.
https://docs.media.bitpipe.com/io_11x/io_115656/item_894327/Maintaining%20continuous%20compliance.pdf
[7] Martin Kellogg, Martin Schäf, Serdar Tasiran, and Michael D. Ernst. Continuous Compliance. In ASE '20. 511–523.
[8] Ze Shi Li, Colin Werner, Neil Ernst, and Daniela Damian. 2020. GDPR Compliance in the Context of Continuous Integration. (2020).
[9] Marco Moscher. 2017. Continuous Compliance Testing. Master's thesis.
[10] Simon Phipps and Stefano Zacchiroli. 2020. Continuous Open Source License Compliance. Computer 53, 12 (12 2020), 115–119.
[11] Arstanaly Rysbekov. 2022. Continuous Compliance: DevOps Approach to Compliance And Change Management. Master's thesis.
[12] Ali Shahrokni and Patrizio Pelliccione. 2022. Significance of Continuous Compliance in Automotive. In EASE '22. 272—273.
[13] Andreas Steffens, Horst Lichter, and Marco Moscher. 2018. Towards Data-Driven Continuous Compliance Testing. In SE '18. 78–84.
[14] Fabiola Moyón, Florian Angermeir, and Daniel Mendez. 2024. Industrial Challenges in Secure Continuous Development. In ICSE '24. 3 pages.
[15] Fabiola Moyón, Kristian Beckers, Sebastian Klepper, Philipp Lachberger, and Bernd Bruegge. 2018. Towards continuous security compliance in agile software development at scale. In RCoSE '18. 31–34.
[16] Hela Oueslati, Mohammad Masudur Rahman, and Lotfi ben Othmane. 2015. Literature Review of the Challenges of Developing Secure Software Using the Agile Approach. In ARES '15. 540–547.
[17] Sebastian Nägele, Natalie Schenk, and Florian Matthes. 2023. The Current State of Security Governance and Compliance in Large-Scale Agile Development: A Systematic Literature Review and Interview Study. In CBI '23. 1–10.

Thank you

Contact

Florian Angermeir
fortiss & Blekinge Institute of Technology
angermeir@fortiss.org

Jannik Fischbach
fortiss & Netlight Consulting GmbH
fischbach@fortiss.org

Fabiola Moyón
Siemens Technology & Technical University of Munich
fabiola.moyon@siemens.com

Daniel Mendez
Blekinge Institute of Technology & fortiss
daniel.mendez@bth.se

Resources

Preprint
https://arxiv.org/pdf/2407.21494

DOI
https://dl.acm.org/doi/10.1145/3674805.3690748

Auxiliary Material
https://figshare.com/articles/dataset/Online_Material/25199225/1