

Representing Global DevSecOps to Usefully Support Software Engineering Practice

Gavin Zhao

PhD Candidate

School of Engineering, Computer and Mathematical Sciences
Faculty of Design & Creative Technologies
Auckland University of Technology
City Campus, Auckland, New Zealand
Email: gavin.zhao@autuni.ac.nz



CONTENTS

① Key Concepts

- DevOps
- Security
- DevSecOps
- GSE

③ MLR on DevSecOps

- MLR search
- Thematic analysis
- MLR results
- DevSecOps models
- Publications

② Research Design

- Research goals
- Research questions
- Research methods:
MLR + Delphi study

④ Delphi study

- Preparing
- Conducting
- Analyzing
- Delphi vs MLR Results
- Local vs Global



1. Key Concepts – DevOps

DevOps can be defined as a software process, methodology, movement, even a culture, aimed at bridging the gap between Development (Dev) and Operations (Ops).



DevOps

Why DevOps?

- gap between Dev & Ops getting closer along with the adoption of clouds, micro-services, and containers;
- better collaboration and teamwork between Dev & Ops;
- faster development and easier deployment by CI/CD;
- higher effectiveness by automation;
- higher product quality and greater business value.



1. Key Concepts – Security in SE



Security

- Security is an important non-functional requirement of software development but is often devalued in DevOps programs.
- It includes security of the software development environment (security threats in the factory) and security of the software being developed (software security testing)
- Growing importance of security includes privacy to users in larger scale systems, SaaS, globally distributed systems, and its conflicts with rapid delivery cycles.
- Use of containers, cloud and server-less computing brings increasing security complications.



1. Key Concepts – DevSecOps

DevSecOps/SecDevOps is created as a security-orientation expansion to DevOps for integrating security into DevOps by improving the collaboration between development, operation and security teams.



DevSecOps

Benefits:

- shifts security to the early stages (shift-left);
- carries out continuous security in the entire Software Development Lifecycle (SDLC);
- employs automation to reduce the need for manual security support.



1. Key Concepts – Global Software Engineering

Global Software Engineering (GSE) is a business strategy aimed to find specialized and diverse resources by accessing “a global pool” of skilled human resources, to improve competitiveness by accessing a global market.



GSE

Benefits:

- reduce costs due to possible salary savings
- shorten duration due to time-zone effectiveness and round-the-clock productivity



1. Key Concepts – Global Software Engineering

GSE depends on distributed teams with stakeholders from different locations, different time zones, and even different organizational and national cultures.



GSE faces challenges from geographical, temporal, linguistic and cultural distances so that it is particularly associated with the 3C Collaboration model (Communication, Coordination and Cooperation).

GSE and DevOps/DevSecOps:

They all belong to Collaborative Software Engineering (CoSE), which is about creating the organizational structures, reward structures, and work breakdown structures that afford effective work towards the goal.



2. Research Design – Research Goals

Research Objectives / Potential Contributions:

- to observe, document and analyze the current state of DevSecOps;
- to compare the differences between local and global DevSecOps;
- to develop a conceptual framework for global DevSecOps guided by experts in the domains of DevOps, security, and GSE.



2. Research Design – Research Questions

RQ 1

How do the experts prioritize the identified challenges, practices, tools and metrics of DevSecOps?

Sub-question 1.1. What additional DevSecOps challenges, practices, tools and metrics could be collected from the experts?

Sub-question 1.2. Will the experts have 'dissent' opinions on the prioritization due to their different roles, e.g. academic, industrial, technical and managerial.

RQ 2

What are the experts' opinions on DevSecOps in GSE contexts?

Sub-question 2.1. How is it different between local and global settings?

Sub-question 2.2. What additional challenges, practices, tools and metrics when it comes to a global setting?



3. MLR on DevSecOps – What is MLR



Multi-vocal Literature Review (MLR) : is a special form of systematic literature review which does not only use formally published literature (WL) but also includes unpublished work (GL).

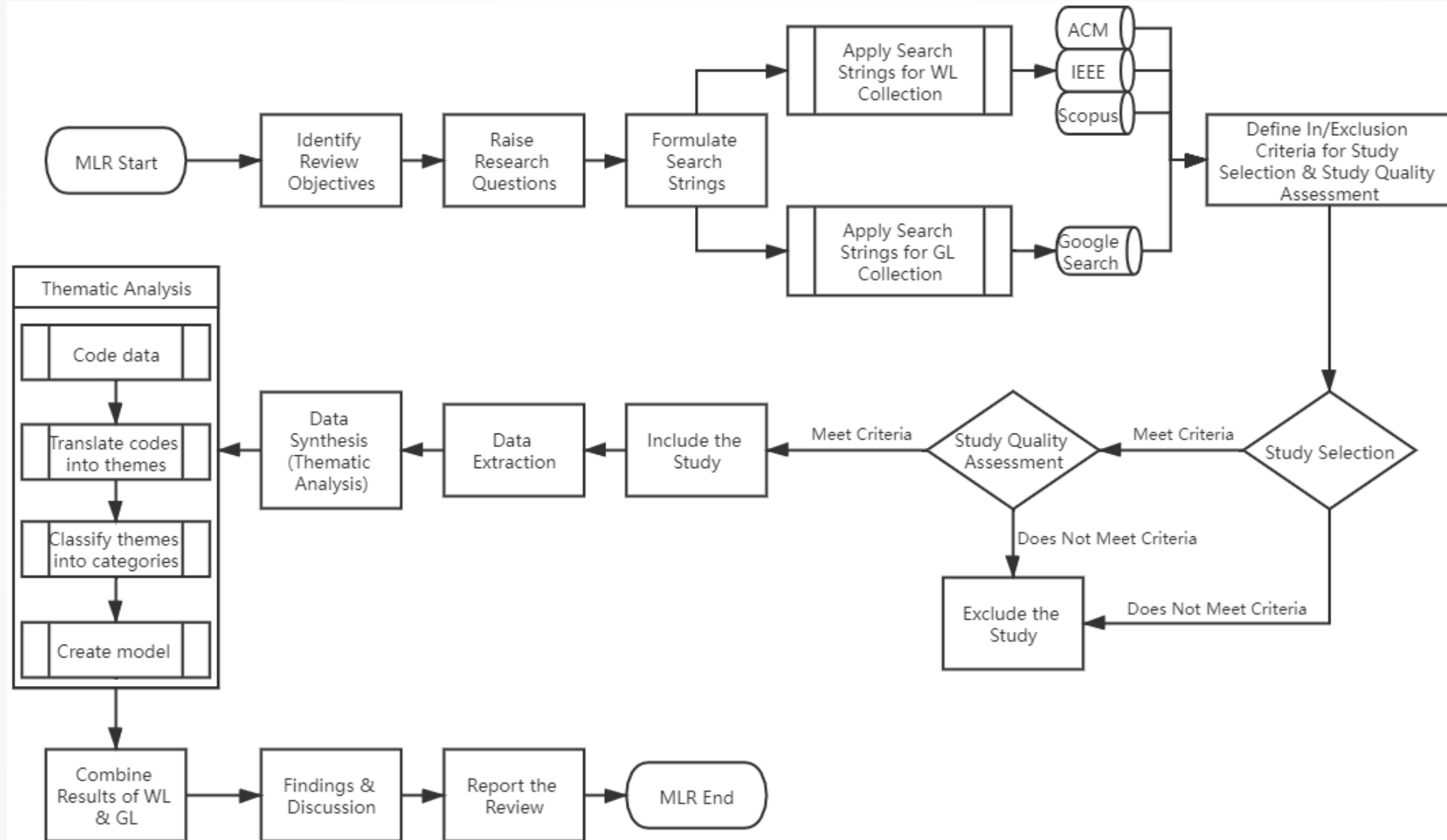
- White Literature (WL): formally published literature, e.g. journal articles and conference papers.
- Grey Literature (GL): unpublished work, e.g. technical reports, websites, blog posts, etc.

Reason for using MLR:

DevSecOps is an increasingly topical concept in both academic and industrial settings, the voices from academia and industry are equally essential.



3. MLR on DevSecOps – MLR Process





3. MLR on DevSecOps – MLR Search

*Search String 1 = "DevOps" AND ("security" OR "secure" OR "safe")
OR "SecDevOps" OR "DevSecOps"*

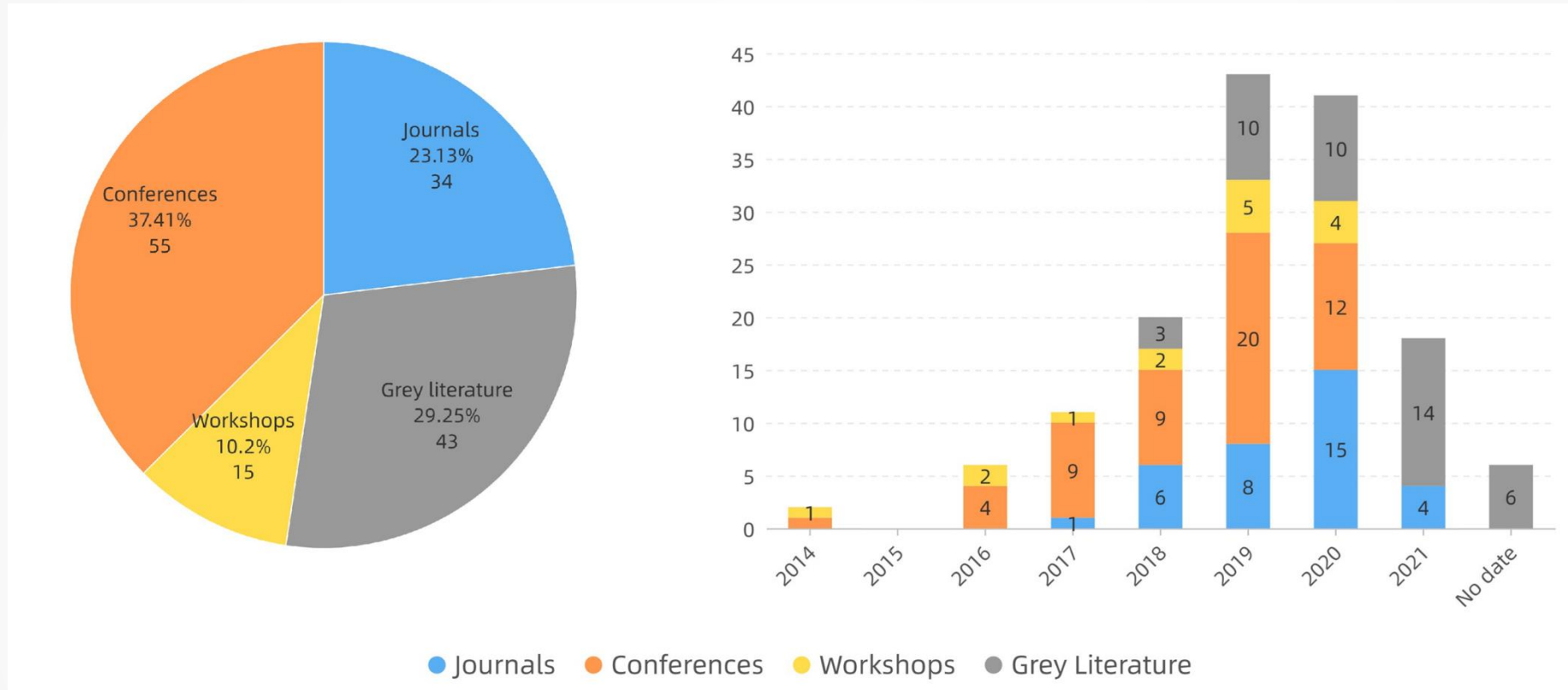
*Search String 2 = "DevOps" AND ("security" OR "secure" OR "safe") AND ("global
software engineering" OR "global software development" OR "GSE" OR "GSD" OR
"globally distributed software*") OR "SecDevOps" OR "DevSecOps"*

Summary of MLR search execution		
Search Steps	Search 1 Results	Search 2 Results
	WL / GL	WL / GL
Applying Search String	327 / 180 studies	90 / 100 studies
Study Pre-selection	238 / 56 studies	66 / 3 studies
Study Selection and QA	112 (acm-28, ieee-46, scopus-38) / 42 studies	2 (acm-2) / 0 study

Lack of global dimension of DevSecOps in the existing literature

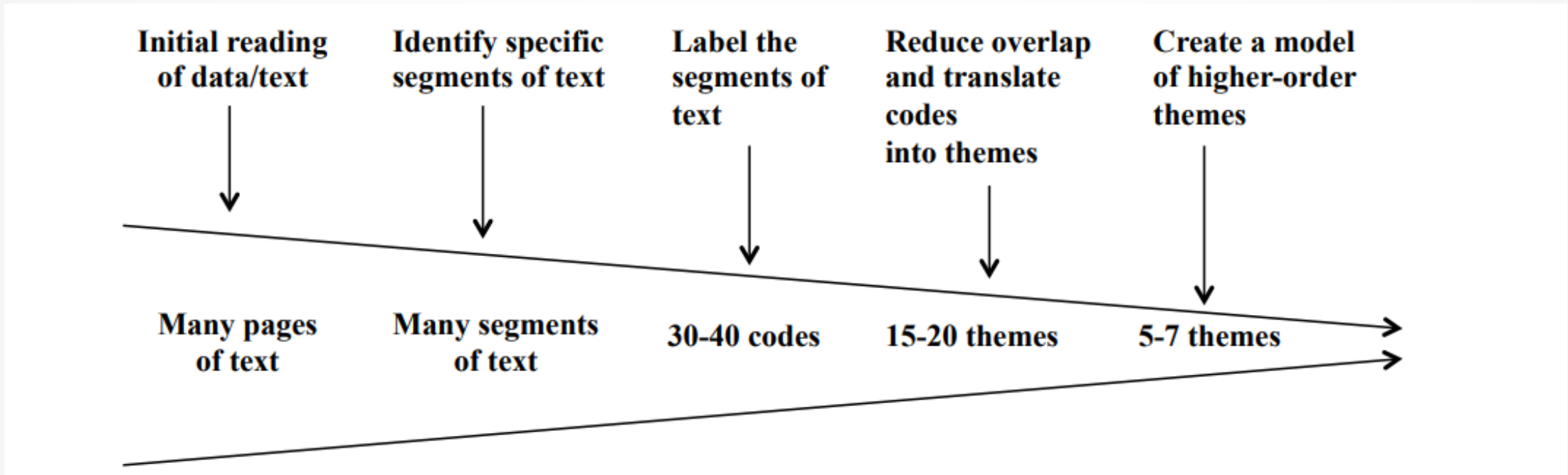


3. MLR on DevSecOps – MLR Search



Number of included papers based on source types and published years

3. MLR on DevSecOps – Thematic Analysis



Thematic Analysis (TA) is a method for identifying, analyzing and reporting themes with qualitative data.



3. MLR on DevSecOps – Thematic Analysis

Thematic analysis and synthesis results

Source	Extract data	Code data	Translate codes into themes	Classify themes into categories
WL	33 DevSecOps definitions	49 codes	14 themes	4 categories: OPC, PC, Technology, Business
	106 DevSecOps challenges	74 codes	36 themes	4 categories: OPC, PC, Technology, Business
	267 DevSecOps practices	86 codes	41 themes	3 categories: OPC, PC, Technology
	16 DevSecOps metrics	41 codes	15 themes	4 categories: OPC, PC, Technology, Business
	33 DevSecOps tools	33 codes	11 themes	Single category: Technology
GL	15 DevSecOps definitions	35 codes	20 themes	4 categories: OPC, PC, Technology, Business
	54 DevSecOps challenges	49 codes	16 themes	3 categories: OPC, PC, Technology
	143 DevSecOps practices	106 codes	54 themes	4 categories: OPC, PC, Technology, Business
	6 DevSecOps metrics	16 codes	6 themes	2 categories: PC, Business
	45 DevSecOps tools	45 codes	14 themes	Single category: Technology

Themes were classified into four categories:

- Organization, People & Culture (OPC)
- Process Capabilities (PC)
- Technology
- Business



3. MLR on DevSecOps – MLR Results

To the knowledge, we find that most of existing literature only contains two of the three terms:

- DevOps + Security (DevSecOps), no GSE;
- DevOps + GSE (global DevOps), no Security.

Absence of global

Reasons:

- no differences between local and global DevSecOps;
- security is a centralized and control-oriented function in organizations, so global aspects are not prominent;
- construction of search string;
- research gap in this direction.



3. MLR on DevSecOps – MLR Results

Key Findings

- Five major aspects of DevSecOps have been identified in the included (white and grey) literature: **Definitions, Challenges, Practices, Tools/Technologies, Metrics/Measurement**.
- Related **themes** of each aspect have been collected and analyzed by performing a **Thematic Analysis (TA)** process.
- A **Challenge-Practice-Tool-Metric (CPTM) model** for DevSecOps has been built by integrating the themes of the latter four aspects.
- The **absence of global DevSecOps** has been identified.

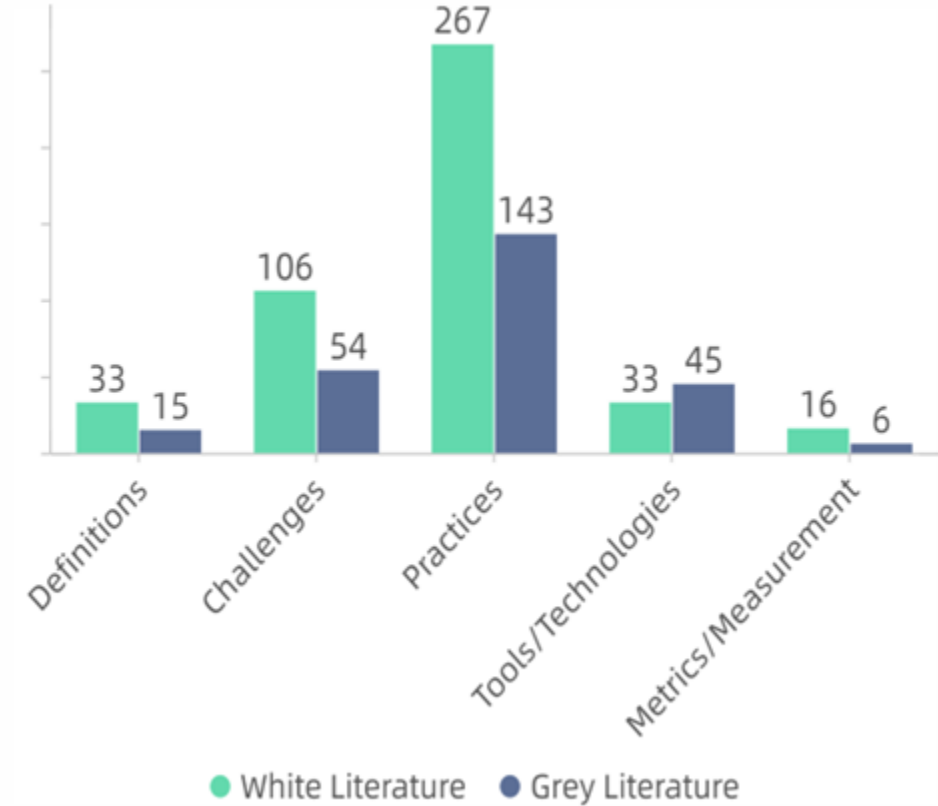


3. MLR on DevSecOps – MLR Results

Five aspects of DevSecOps have been identified in the literature:

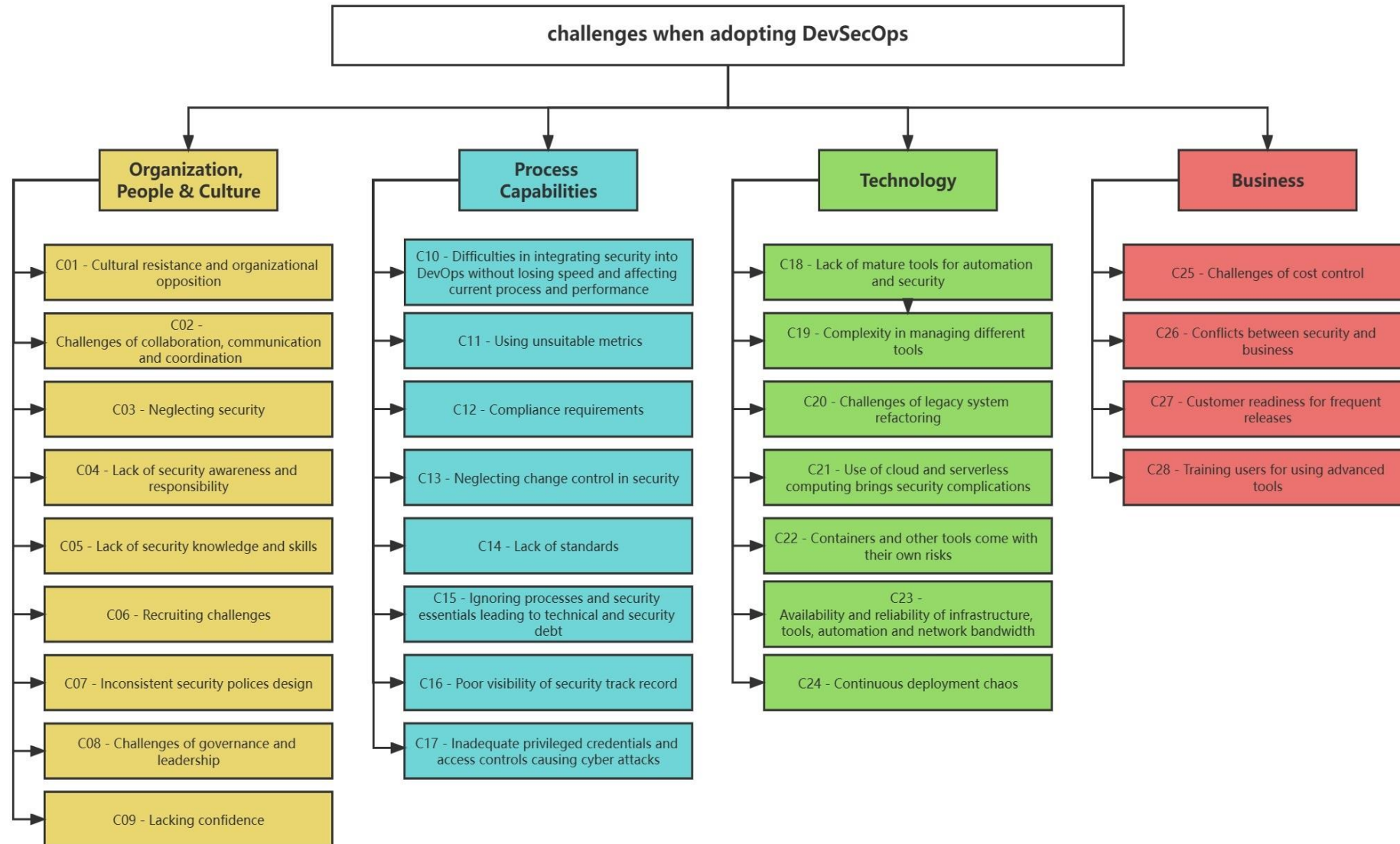
- **Definitions:** definitions for the term “DevSecOps” and equivalent terms;
- **Challenges:** problems, concerns and uphill tasks that are faced during implementing DevSecOps;
- **Practices:** DevOps and security activities suited for DevSecOps;
- **Tools/Technologies:** specific tools and technological approaches that can be used for DevSecOps;
- **Metrics/Measurement:** means for measuring security level and DevSecOps maturity.

In comparison of WL and GL results (academic and industrial), WL contributes more to phenomenological researches, defining concepts and identifying DevSecOps challenges and practices; GL contributes more to the business perspective, focusing on practical DevSecOps tools and metrics to provide solutions.





3. MLR on DevSecOps – MLR Results



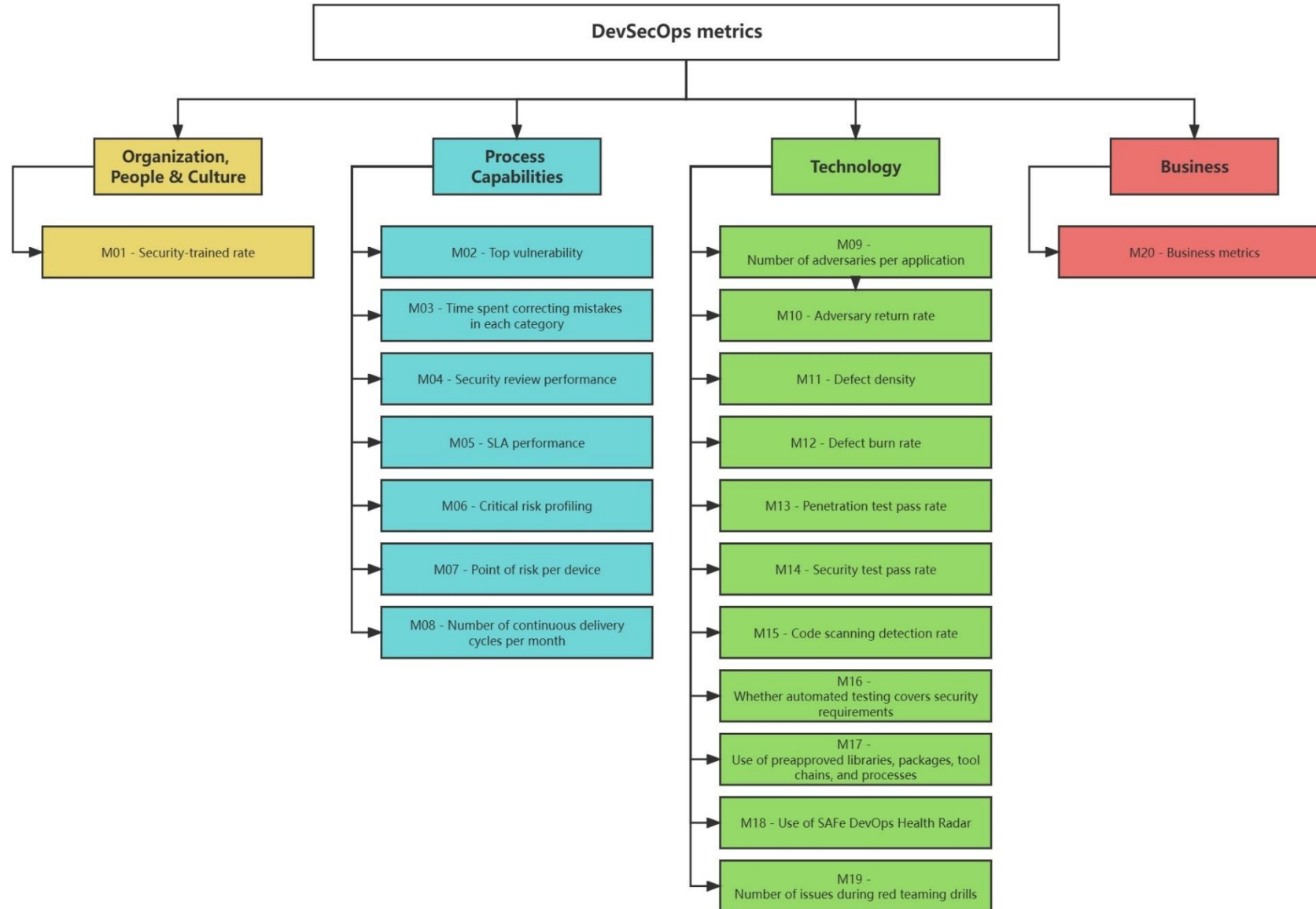


3. MLR on DevSecOps – MLR Results



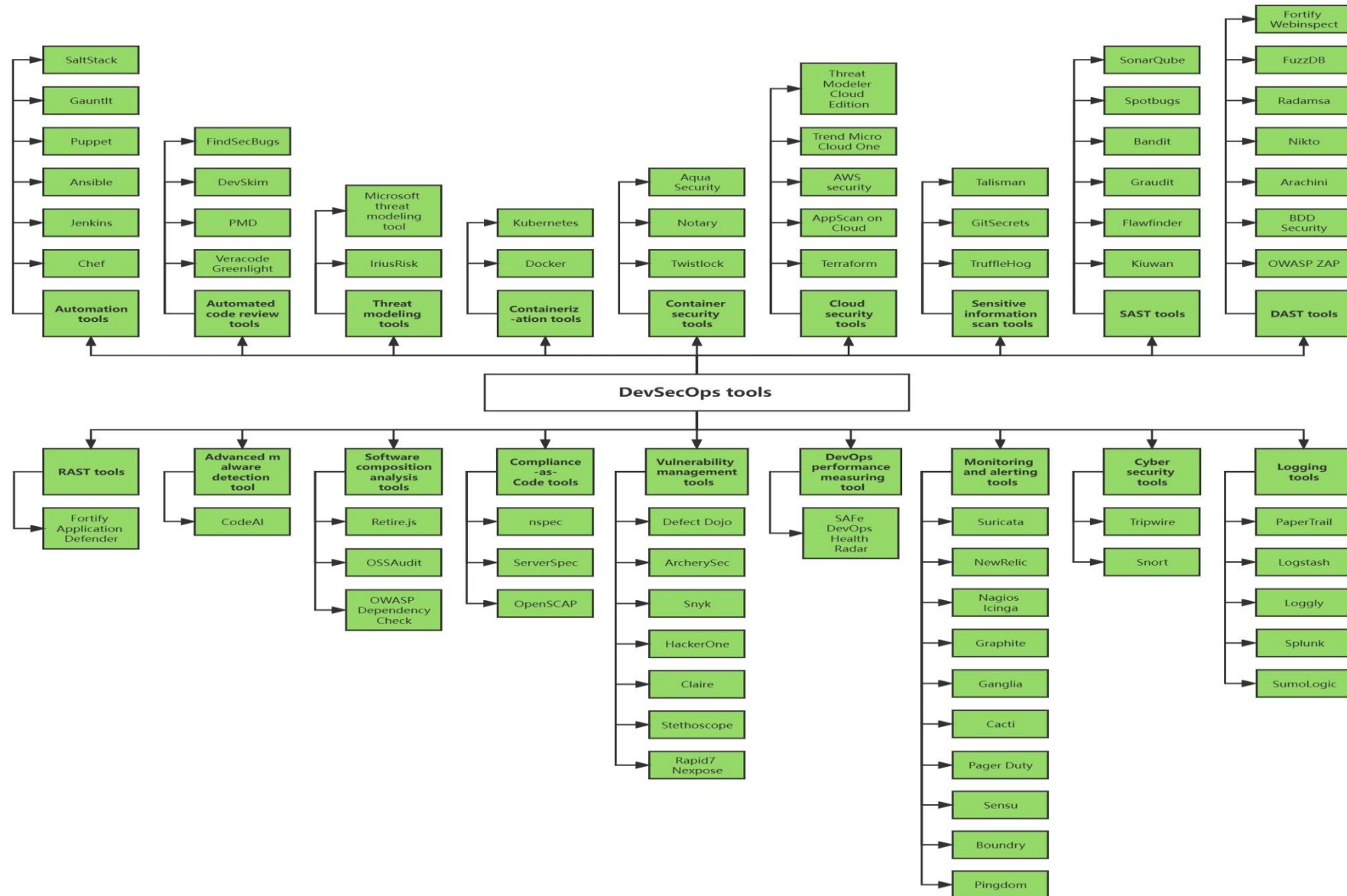


3. MLR on DevSecOps – MLR Results

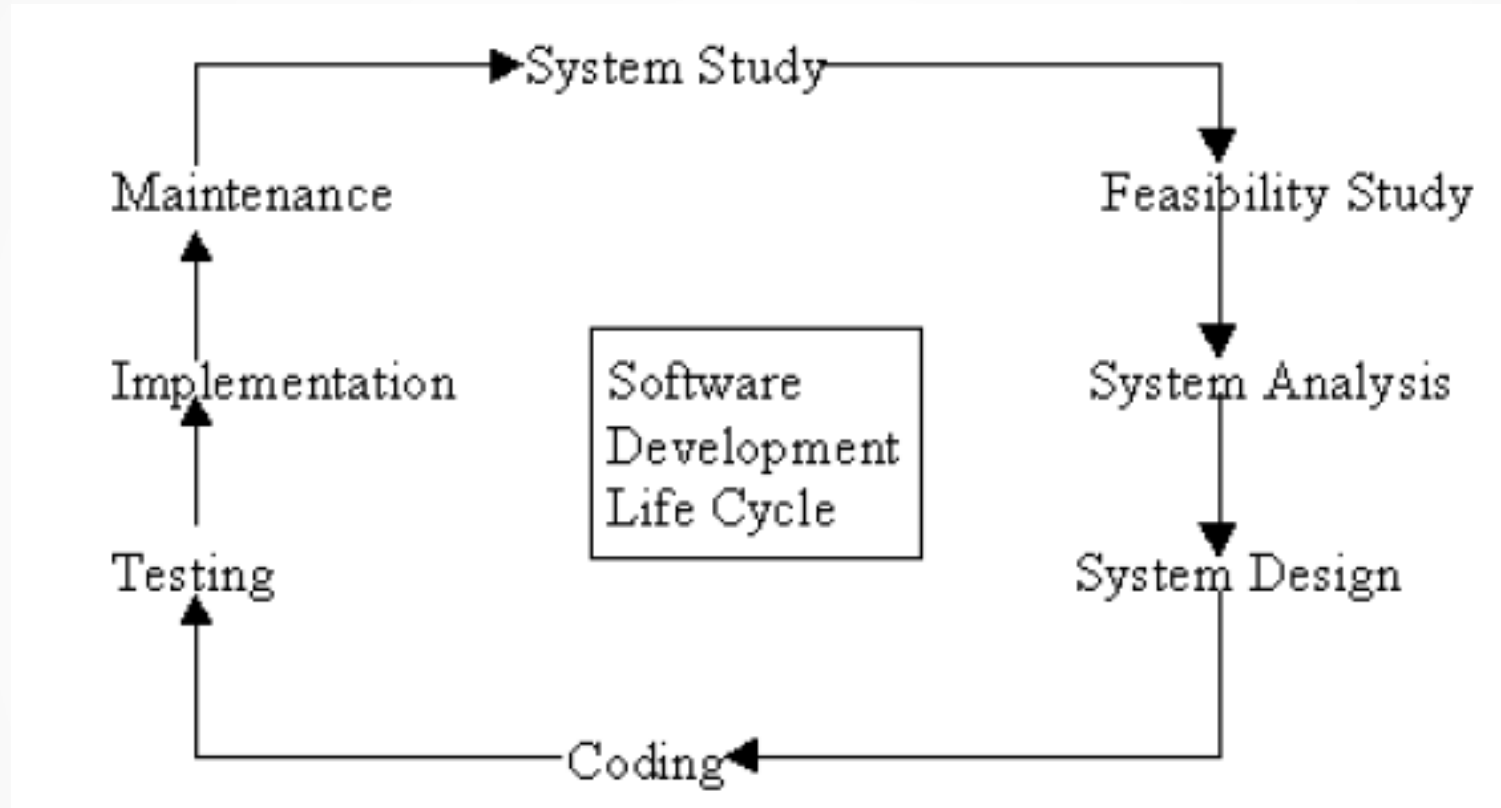




3. MLR on DevSecOps – MLR Results



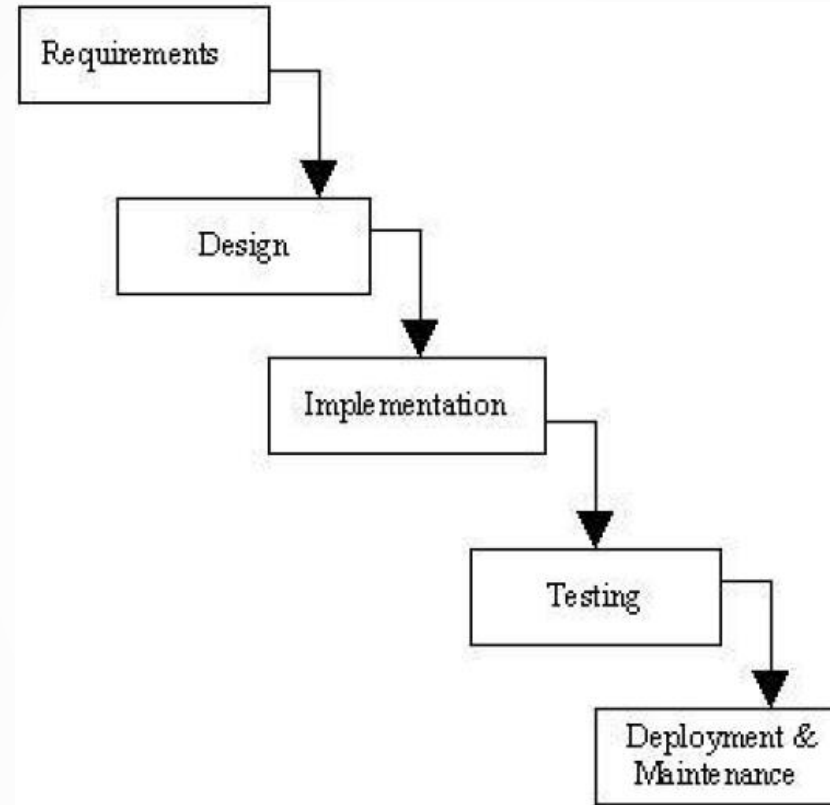
3. MLR on DevSecOps – Common SDLC Model



Common Steps in a Software Development Lifecycle (SDLC) Model



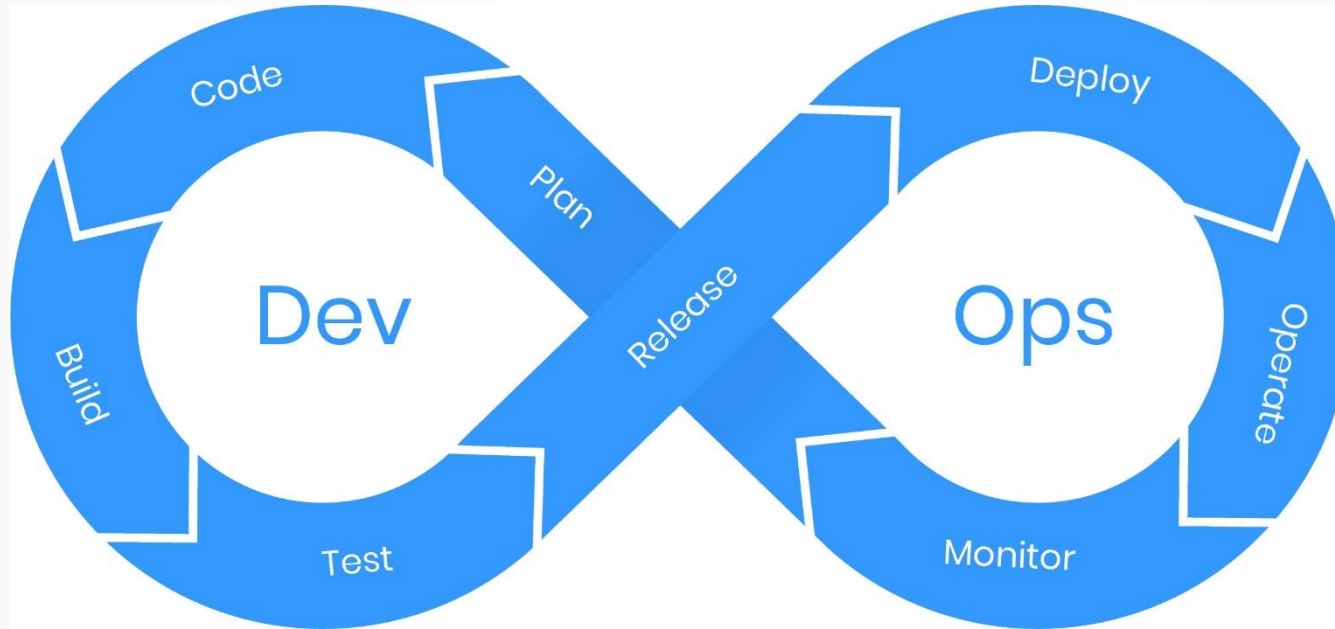
3. MLR on DevSecOps – Waterfall Model



Waterfall Model

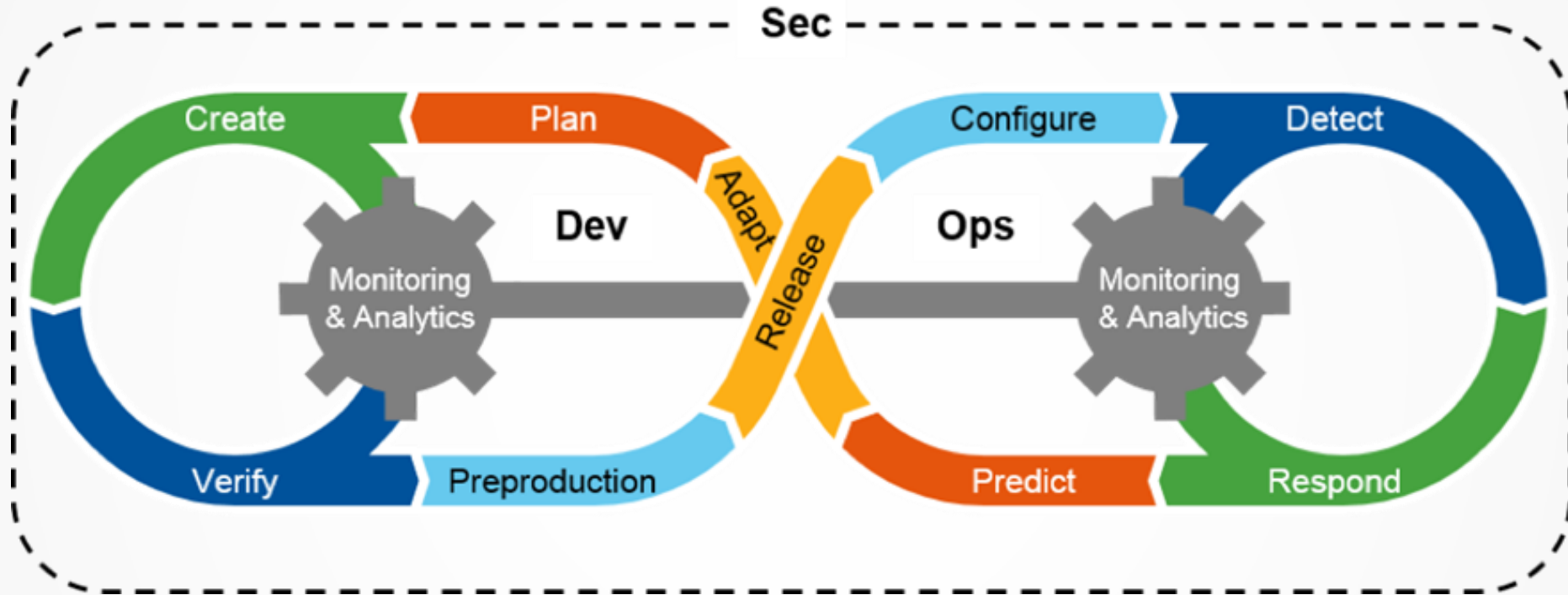


3. MLR on DevSecOps – DevOps Model



DevOps Model by Jireh Tech

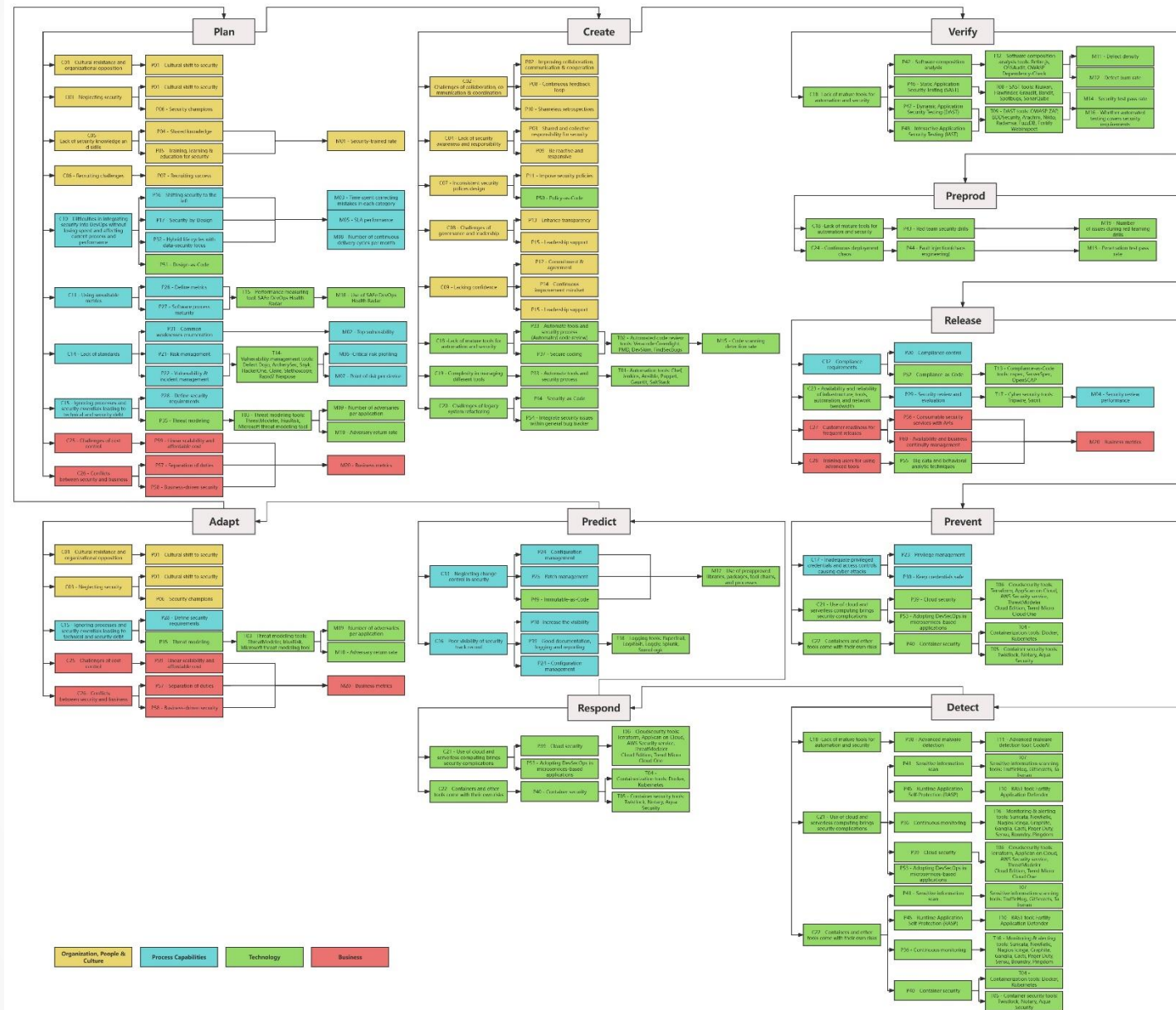
3. MLR on DevSecOps – DevSecOps Model



DevSecOps Model by Gartner




3. MLR on DevSecOps – CPTM Model by us





3. MLR on DevSecOps – Our Publication


The Journal of Systems and Software 214 (2024) 112063



Contents lists available at [ScienceDirect](#)

The Journal of Systems & Software


journal homepage: www.elsevier.com/locate/jss



Identifying the primary dimensions of DevSecOps: A multi-vocal literature review[☆]

Xiaofan Zhao^{*}, Tony Clear, Ramesh Lal

Auckland University of Technology, 55 Wellesley Street East, Auckland Central, Auckland, New Zealand



ARTICLE INFO

Dataset link: <https://doi.org/10.5281/zenodo.7959584>

Keywords:

Multivocal literature review

DevSecOps

DevOps

Security

Global software engineering

ABSTRACT

Context: Security as a key non-functional requirement of software development is often ignored and devalued in DevOps programs, with security seen as an inhibitor to high velocity required in DevOps implementation. Hence, the DevSecOps approach as a security-orientated expansion to DevOps, has aimed to integrate security into DevOps implementation by promoting collaboration among development, operation and security teams. DevSecOps is a topical concept and rapidly emerging area of practice in both academic and industrial settings.

Objective: We reviewed both the white and grey literature to identify recent researches and practical trends of DevSecOps, aiming to: (a) review, document and analyze the current state of DevSecOps in the existing literature; (b) investigate the application of DevSecOps in Global Software Engineering (GSE) contexts.

Method: A Multi-vocal Literature Review on DevSecOps and its global application was conducted, by executing a dual-track strategy including white (104 studies) and grey (43 studies) literature from 2012 to 2021. A Thematic Analysis was performed to identify, synthesize and analyze the themes within data for reporting the MLR results.

Results: Through the Multi-vocal Literature Review and Thematic Analysis, this paper identifies five major aspects of DevSecOps (Definitions, Challenges, Practices, Tools/Technologies, and Metrics/Measurement); collects related themes of each aspect; and generates a **Challenge-Practice-Tool-Metric (CPTM) model** by integrating the themes of the latter four aspects within a lifecycle model. Moreover, an unexplored area relating to the global application of DevSecOps has been identified.

Conclusion: Based on MLR results, a CPTM (Challenge-Practice-Tool-Metric) model is built to reveal the current status of DevSecOps. The model provides a breakdown and a broad landscape of DevSecOps, from which researchers and practitioners may select an area of focus to improve their knowledge or practice. With DevSecOps spanning the many stages of the lifecycle, we believe the model will enable emphases and absences such as global aspects to be investigated.

Editor's note: Open Science material was validated by the Journal of Systems and Software Open Science Board.

28



4. Delphi Study on DevSecOps – What is Delphi

Delphi (aka expert survey method) is a data collection method to solicit opinions from experts in certain domains by conducting multiple rounds of interview/survey, aiming to generate insights and get consensus on controversial subjects with limited information. The key differences between ordinary surveys and Delphi method are the iteration and the use of the feedback.

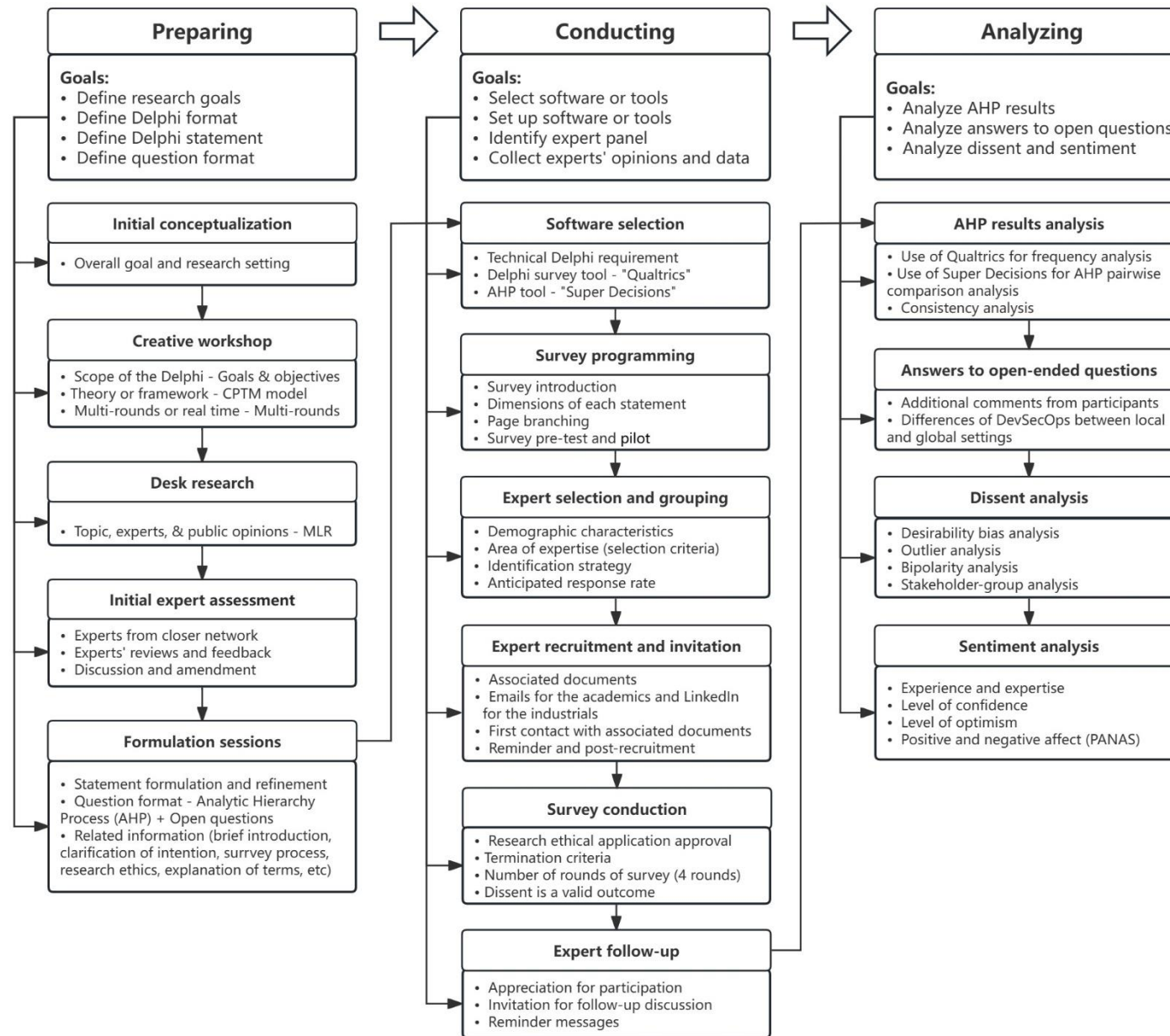
Delphi Study

Benefits (reasons for selecting Delphi):

- Delphi is best suited for developing new concepts and setting the unexplored directions (absence of global DevSecOps in MLR);
- Online surveys with international experts in anonymous format, without geographical restriction;
- Delphi is often used for testing and improving a set of outcomes from literature review, that's exactly what happened to this research.

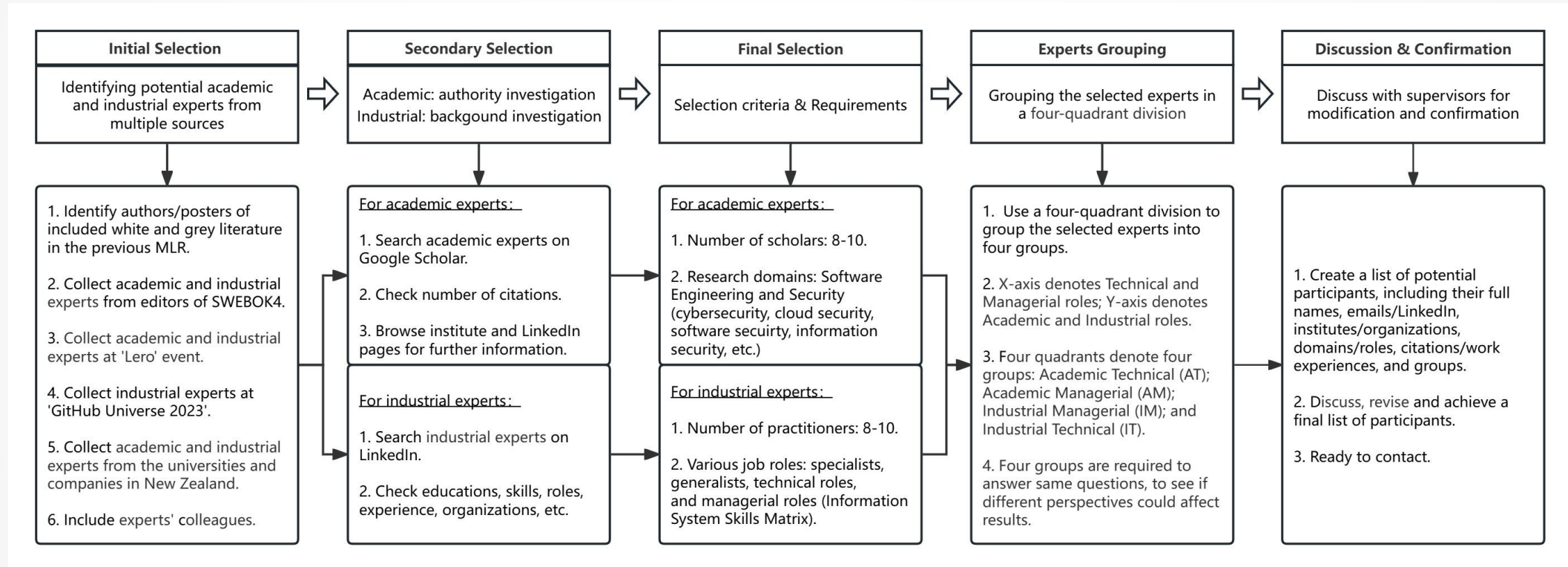


4. Delphi Study – Process





4. Delphi Study – Expert Selection



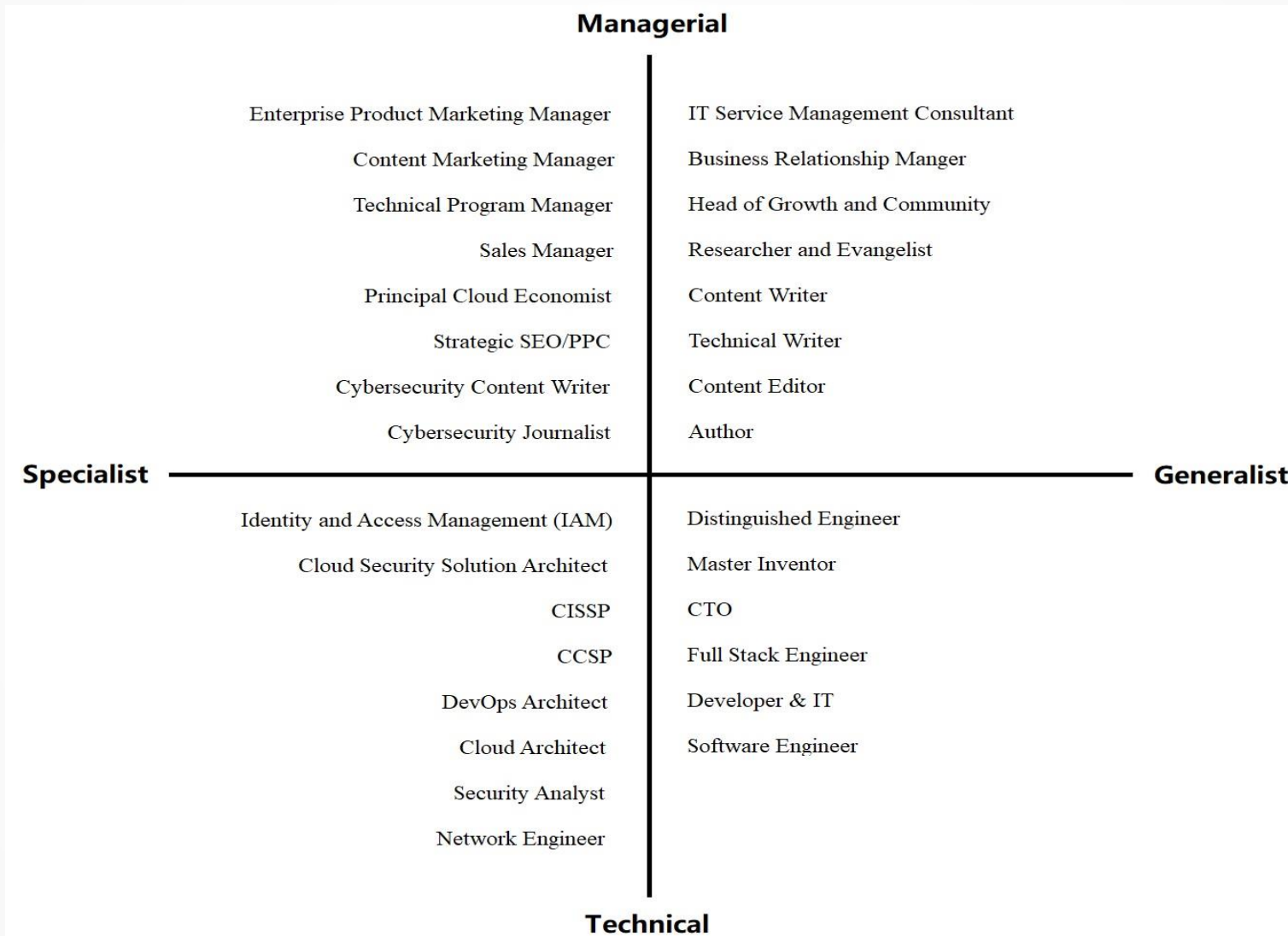


4. Delphi Study – Expert Selection Criteria

Criteria↵	Requirements↵
Number of experts↵	Minimum of 20 experts.↵
Professional experience↵	Minimum 5 years.↵
Field of work↵	<ul style="list-style-type: none">• Academia: 10-15 experts.↵• Industry: 10-15 experts (various roles).↵• Non-profit organizations (NPO): No formal number required.↵• Overlapped fields: No formal number required.↵
Domain of expertise↵	Academia: Software Engineering (SE) and Information Security (IS)↵ Industry: various job roles in the Information System Skills Matrix (specialist, generalists, technical roles, and managerial roles)↵



4. Delphi Study – Industrial Expert Roles





4. Delphi Study – Survey Conduct

Round of survey↵	Estimated duration↵	Goal and activities↵	↵
Round One↵	15 minutes↵	Rate the importance of identified DevSecOps challenges↵	↵
Round Two↵	20 minutes↵	Assess the revised challenges (minimize the number of comparisons to reduce time and avoid inconsistency);↵ Rate the importance/adoption of identified DevSecOps practices↵	↵
Round Three↵	30 minutes↵	Assess the revised practices (minimize the number of comparisons to reduce time and avoid inconsistency);↵ Rate the importance/adoption of identified DevSecOps tools and metrics.↵	↵
Round Four↵	20 minutes↵	Assess the revised tools and metrics;↵ Assess the refined CPTM model (open questions).↵	↵



4. Delphi Study – Analyzing (Challenges)

DevSecOps Challenge	Category of Challenges	Category Normalized Value	Challenge Normalized Value within Category	Ranking within Category	Overall Priority	Overall Ranking
C01-Cultural resistance and organizational opposition	OPC	0.551570177	0.055256975	8	0.0304781	12
C02-Challenges of collaboration, communication and coordination	OPC	0.551570177	0.059057908	7	0.032574581	11
C03-Neglecting security	OPC	0.551570177	0.115978761	5	0.063970426	6
C04-Lack of security awareness and responsibility	OPC	0.551570177	0.211032393	1	0.116399174	1
C05-Lack of security knowledge and skills, need for training	OPC	0.551570177	0.131483634	4	0.072522451	4
C06-Recruiting challenges	OPC	0.551570177	0.147661027	2	0.081445419	2
C07-Inconsistent security policies design	OPC	0.551570177	0.114243675	6	0.063013404	7
C08-Challenges of governance and leadership	OPC	0.551570177	0.138017136	3	0.076126136	3
C09-Lacking confidence	OPC	0.551570177	0.027268491	9	0.015040487	21
C10-Difficulties in integrating security into DevOps without losing speed and affecting current process and performance	PC	0.234334769	0.071004516	6	0.016638827	19
C11-Using unsuitable metrics	PC	0.234334769	0.035989662	8	0.008433629	26
C12-Compliance requirements	PC	0.234334769	0.156604968	3	0.036697989	10
C13-Neglecting change control in security	PC	0.234334769	0.116865132	4	0.027385564	13
C14-Lack of standards	PC	0.234334769	0.083647625	5	0.019601547	17
C15-Ignoring processes and security essentials leading to technical and security debt	PC	0.234334769	0.190502711	2	0.044641409	9
C16-Poor visibility of security track record	PC	0.234334769	0.067877958	7	0.015906166	20
C17-Inadequate privileged credentials and access controls causing cyber attacks	PC	0.234334769	0.277507429	1	0.065029639	5
C18-Lack of mature tools for automation and security	Technology	0.091299172	0.138395784	4	0.01263542	24
C19-Complexity in managing different tools	Technology	0.091299172	0.15628105	3	0.01426833	22
C20-Challenges of legacy system refactoring	Technology	0.091299172	0.267836211	1	0.024453224	15
C21-Use of cloud and serverless computing brings security complications	Technology	0.091299172	0.076141135	6	0.006951623	27
C22-Containers and other tools come with their own risks	Technology	0.091299172	0.057907956	7	0.005286948	28
C23-Availability and reliability of infrastructure, tools, automation, and network bandwidth	Technology	0.091299172	0.183943479	2	0.016793887	18
C24-Continuous deployment chaos	Technology	0.091299172	0.119494386	5	0.010909738	25
C25-Challenges of cost control	Business	0.122795882	0.107909667	4	0.013250863	23
C26-Conflicts between security and business	Business	0.122795882	0.480364189	1	0.058986744	8
C27-Customer readiness for frequent releases	Business	0.122795882	0.215819334	2	0.026501725	14
C28-Training users for using advanced tools	Business	0.122795882	0.19590681	3	0.024056549	16



4. Delphi Study – Analyzing (Challenges)

DevSecOps Challenge	Category of Challenges	Category Total Frequency in MLR	Frequency in MLR	Ranking within Category in MLR	Overall Ranking in MLR
C01-Cultural resistance and organizational opposition	OPC	42	7	3	6
C02-Challenges of collaboration, communication and coordination	OPC	42	20	1	2
C03-Neglecting security	OPC	42	3	4	9
C04-Lack of security awareness and responsibility	OPC	42	3	5	10
C05-Lack of security knowledge and skills, need for training	OPC	42	9	2	5
C06-Recruiting challenges	OPC	42	3	6	11
C07-Inconsistent security policies design	OPC	42	2	7	14
C08-Challenges of governance and leadership	OPC	42	1	8	19
C09-Lacking confidence	OPC	42	1	9	20
C10-Difficulties in integrating security into DevOps without losing speed and affecting current process and performance	PC	26	11	1	4
C11-Using unsuitable metrics	PC	26	3	3	12
C12-Compliance requirements	PC	26	5	2	7
C13-Neglecting change control in security	PC	26	1	6	21
C14-Lack of standards	PC	26	2	4	15
C15-Ignoring processes and security essentials leading to technical and security debt	PC	26	1	7	22
C16-Poor visibility of security track record	PC	26	1	8	23
C17-Inadequate privileged credentials and access controls causing cyber attacks	PC	26	2	5	16
C18-Lack of mature tools for automation and security	Technology	50	19	2	3
C19-Complexity in managing different tools	Technology	50	1	6	25
C20-Challenges of legacy system refactoring	Technology	50	4	3	8
C21-Use of cloud and serverless computing brings security complications	Technology	50	21	1	1
C22-Containers and other tools come with their own risks	Technology	50	3	4	13
C23-Availability and reliability of infrastructure, tools, automation, and network bandwidth	Technology	50	1	7	26
C24-Continuous deployment chaos	Technology	50	1	5	24
C25-Challenges of cost control	Business	6	2	1	17
C26-Conflicts between security and business	Business	6	2	2	18
C27-Customer readiness for frequent releases	Business	6	1	3	27
C28-Training users for using advanced tools	Business	6	1	4	28



4. Delphi Study – Analyzing (Delphi vs MLR)

DevSecOps Challenge	Category of Challenges	Category Ranking in MLR	Category Ranking in Delphi	Ranking within Category in MLR	Ranking within Category in Delphi	Overall Ranking in MLR	Overall Ranking in Delphi
C01-Cultural resistance and organizational opposition	OPC	2	1	3	8	6	12
C02-Challenges of collaboration, communication and coordination	OPC	2	1	1	7	2	11
C03-Neglecting security	OPC	2	1	4	5	9	6
C04-Lack of security awareness and responsibility	OPC	2	1	5	1	10	1
C05-Lack of security knowledge and skills, need for training	OPC	2	1	2	4	5	4
C06-Recruiting challenges	OPC	2	1	6	2	11	2
C07-Inconsistent security policies design	OPC	2	1	7	6	14	7
C08-Challenges of governance and leadership	OPC	2	1	8	3	19	3
C09-Lacking confidence	OPC	2	1	9	9	20	21
C10-Difficulties in integrating security into DevOps without losing speed and affecting current process and performance	PC	3	2	1	6	4	19
C11-Using unsuitable metrics	PC	3	2	3	8	12	26
C12-Compliance requirements	PC	3	2	2	3	7	10
C13-Neglecting change control in security	PC	3	2	6	4	21	13
C14-Lack of standards	PC	3	2	4	5	15	17
C15-Ignoring processes and security essentials leading to technical and security debt	PC	3	2	7	2	22	9
C16-Poor visibility of security track record	PC	3	2	8	7	23	20
C17-Inadequate privileged credentials and access controls causing cyber attacks	PC	3	2	5	1	16	5
C18-Lack of mature tools for automation and security	Technology	1	4	2	4	3	24
C19-Complexity in managing different tools	Technology	1	4	6	3	25	22
C20-Challenges of legacy system refactoring	Technology	1	4	3	1	8	15
C21-Use of cloud and serverless computing brings security complications	Technology	1	4	1	6	1	27
C22-Containers and other tools come with their own risks	Technology	1	4	4	7	13	28
C23-Availability and reliability of infrastructure, tools, automation, and network bandwidth	Technology	1	4	7	2	26	18
C24-Continuous deployment chaos	Technology	1	4	5	5	24	25
C25-Challenges of cost control	Business	4	3	1	4	17	23
C26-Conflicts between security and business	Business	4	3	2	1	18	8
C27-Customer readiness for frequent releases	Business	4	3	3	2	27	14
C28-Training users for using advanced tools	Business	4	3	4	3	28	16



4. Delphi Study – Analyzing (Local vs Global)

How does DevSecOps differ in local and global settings?

Opinion	Proportion
Extremely different	7.7%
Slightly different	53.8
Not different	30.8%
Uncertain	7.7%

Differences between local and global DevSecOps

- ✧ It amplifies challenges in team collaboration and communication.
- ✧ More remote work, less direct communication, more ease of misunderstanding, increased communication needs in writing.
- ✧ Synchronization/Coordination between remote teams.
- ✧ Risks/Threats spanning multiple regions.
- ✧ Independent development can propagate risks in a non-uniform way.
- ✧ Issues of data residency, for example, different nation's regulations about personal data can complicate things more than if everything is done in a single country/region.
- ✧ Everyone views DevSecOps differently. Such phenomenal magnified in global settings compared to what we see in local settings.
- ✧ Disagreements on best practices.
- ✧ Compliance with external regulations worldwide.
- ✧ Business focus and level of importance is different.



References

- [1] W. Hussain, T. Clear, S. MacDonell, Emerging trends for global devops: A new zealand perspective, in: 2017 IEEE 12th International Conference on Global Software Engineering, IEEE, 2017, pp. 21–30. doi:10.1109/icgse.2017.16.
- [2] H. Myrbakken, R. Colomo-Palacios, Devsecops: A multivocal literature review, in: Software Process Improvement and Capability Determination, Vol. 770, Springer, Cham, 2017, pp. 17–29. doi:10.1007/525 978-3-319-67383-7_2.
- [3] K. Carter, Francois raynaud on devsecops, IEEE Software 34 (5) (2017) 93–96. doi:10.1109/ms.2017.3571578.
- [4] Z. Ahmed, S. C. Francis, Integrating security with devsecops: Techniques and challenges, in: 2019 International Conference on Digitization, IEEE, 2019, pp. 178–182. doi:10.1109/icd47981.2019.9105789.
- [5] V. Garousi, M. Felderer, M. M`antyl`a, Guidelines for including grey literature and conducting multivocal literature reviews in software engineering, Information and Software Technology 106 (2019) 101–121. doi: 10.1016/j.infsof.2018.09.006.
- [6] P. Chestna, Appsec in a devops world (2016). URL <https://owasp.org/www-pdf-archive/2017-04-20-AppSecDevops.pdf>
- [7] J. Whitehead, I. Mistrik, J. Grundy, A. van der Hoek, Collaborative Software Engineering: Concepts and Techniques, Springer, 2010, pp. 1–30, (inbook). doi:10.1007/978-3-642-10294-3.<https://doi.org/10.1016/j.infsof.2012.05.002>
- [8] A. Vizcaíno, F. Garcíia, M. Piattini, S. Beecham, A validated ontology for global software development, Computer Standards and Interfaces 46 (2016) 66–78. doi:10.1016/j.csi.2016.02.004.
- [9] E. O. Conchuir, P. J. °Agerfalk, H. H. Olsson, B. Fitzgerald, Global software development: Where are the benefits?, CACM 52 (8) (2009) 127–131. doi:10.1145/1536616.1536648.
- [10] Lip-Wah Ho, Tek-Tjing Lie, Paul TM Leong, and Tony Clear. 2018. Developing offshore wind farm siting criteria by using an international Delphi Method. *Energy Policy* 113: 53–67. <http://doi.org/10.1016/j.enpol.2017.10.049>
- [11] D. S. Cruzes, T. Dyba, Recommended steps for thematic synthesis in software engineering, in: 2011 International Symposium on Empirical Software Engineering and Measurement, IEEE, 2011, pp. 275–284. doi:10.1109/ESEM.2011.36.



References

- [12] Orli Weiser, Yoram M. Kalman, Carmel Kent, and Gilad Ravid. 2022. 65 competencies. *Communications of the ACM* 65, 3: 58–66. <http://doi.org/10.1145/3467018>
- [13] Daniel Beiderbeck, Nicolas Frevel, Heiko A. von der Gracht, Sascha L. Schmidt, and Vera M. Schweitzer. 2021. Preparing, conducting, and analyzing Delphi Surveys: Cross-disciplinary practices, New Directions, and advancements. *MethodsX* 8: 101401. <http://doi.org/10.1016/j.mex.2021.101401>
- [14] A. Mishra, D. Dubey, Ga comparative study of different software development life cycle models in different scenarios, *IJARCSMS* 1 (5) (2013) 64–69.
- [15] J. Tech, What is devops. URL <http://www.jirehtechconsulting.com/what-is-devops/>
- [16] N. MacDonald, I. Head, Devsecops: How to seamlessly integrate security into devops (2016). URL <https://www.gartner.com/en/documents/3463417>
- [17] V. Braun, V. Clarke, Using thematic analysis in psychology, *Qualitative Research in Psychology* 3 (2) (2006) 77–101. doi: 10.1191/1478088706qp063oa.
- [18] V. Braun, V. Clarke, Thematic analysis: a reflexive approach (2020). URL <https://www.psych.auckland.ac.nz/en/about/thematic-analysis.html>
- [19] V. Braun, V. Clarke, Guidelines for reviewers and editors evaluating thematic analysis manuscripts (2019). URL <https://cdn.auckland.ac.nz/assets/psych/about/our-research/documents/TA%20website%20update%2010.8.17%20review%20checklist.pdf>
- [20] X. Zhao, T. Clear and R. Lal, Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *The Journal of Systems & Software* (2024), doi: <https://doi.org/10.1016/j.jss.2024.112063>.

The end, thanks.

Presenter: Gavin Zhao

School of Engineering, Computer and Mathematical Sciences
Faculty of Design and Creative Technologies
Auckland University of Technology

AUT
UNIVERSITY

NEW ZEALAND