Building Software Applications Securely With DevSecOps: A Socio-Technical Perspective

Rennie Naidoo and Nicolaas Möller
University of Pretoria, Pretoria, South Africa
rennie.naidoo@up.ac.za
nicolaas.möller@up.ac.za

Abstract: While continuous real-time software delivery practices induced by agile software development approaches create new business opportunities for organizations, these practices also present new security challenges in the DevOps environment. DevSecOps attempts to incorporate advanced automated security practices for agility in the DevOps environment. Mainstream perspectives of DevSecOps tend to overlook the collaborative role played by social actors and their relations with technologies in securing software applications in organizations. The first perspective emphasises the use of technologies such as containers, microservices, cryptographic protocols and origin authentication to secure the continuous deployment pipeline. The other dominant perspective focuses almost exclusively on the social aspects such as organizational silos, culture, and team collaboration. Such one-sided perspectives neglect the socio-technical argument that secure software applications from continuous deployment emerges when developers, quality assurers, operators and security experts combine their collective expertise together with DevSecOps technologies. The article presents a socio-technical framework of DevSecOps based on a systematic literature review. The review focused primarily, but not exclusively, on the computing and information systems literature and identified 26 peer reviewed articles from 2016 to 2020 which met the quality criteria and contributed to the analysis. The authors used a critical appraisal checklist and member checking to assess the quality of the articles. The authors then used thematic analysis to develop a comprehensive framework for DevSecOps based on the insights from these articles and a socio-technical lens. The socio-technical framework can be used by practitioners to perform a more holistic analysis of their DevSecOps practices. It highlights the key social and technical themes that underpin the effectiveness of DevSecOps and how insights about these themes can be used by practitioners to improve the instrumental and humanistic goals of DevSecOps. An interdisciplinary approach is proposed to adequately address challenging socio-technical relationships in DevSecOps. Future research can empirically test the importance of the interplay between technology and human activities to improve the overall performance of DevSecOps and other domains in cyber warfare and security.

Keywords: culture, continuous deployment, DevOps, DevSecOps, security, socio-technical

1. Introduction

Agile development practices enable organizations to continuously deliver software products and services. Since agile development teams commit many small and frequent deployments to production, failure to involve the operations team earlier in the software lifecycle tends to become a source of constraint in the software delivery process. DevOps seeks to promote cross-functional collaboration between the development and operations teams. The semi-automation and full automation of build, deployment, and testing tasks is also a critical capability in improving overall software delivery performance. However, organizations adopting DevOps practices often struggle to manage the tensions between the goals of shortening the development cycle and the faster delivery of features pursued by the development teams and the stability goals pursued by the operations teams. Of greater concern, both these teams tend to neglect security vulnerabilities that threat actors can exploit.

Neil MacDonald (2012) of Gartner initially coined the term DevOpsSec to draw attention to the need to incorporate information security within DevOps practices to balance speed, agility, and security. DevSecOps, as it is more commonly known, extends the objective of DevOps by advocating shift left security, security by design and continuous security testing. By integrating the security team with the software development and operations teams, team members can pay joint attention to information security matters throughout the software development lifecycle (Mansfield-Devine, 2018).

The distinctions between terms such as DevOpsSec, DevSecOps and SecDevOps are not clear in the academic literature. In the grey literature, the placement of “Sec” in the term appears to signify the priority given to Security (Myrbakken and Colomo-Palacios, 2017; Mohan and Othmane, 2016; Rahman and Williams, 2016). DevOpsSec is seen to prioritise development and operations at the expense of security. DevSecOps represent an improvement in the security culture but still prioritises development processes. Meanwhile SecDevOps is the ideal term for security evangelists as it prioritises security processes throughout the development lifecycle

(Mohan and Othmane, 2016). In the academic literature, these terms are often used interchangeably, and some authors have found that the term DevSecOps has become increasingly accepted by practitioners (Myrbakken and Colomo-Palacios, 2017).

In DevSecOps, information security is also emphasised early in the development lifecycle. DevSecOps also uses tools to automate the insertion of security features into software applications. Whereas the waterfall model often relied on the use of a single or few tools, Agile, DevOps and DevSecOps transformations involve an overwhelming number of diverse and specialised tools for planning, tracking, automation, and management tasks (Kersten, 2018). A Tasktop survey of 300 Enterprise IT organizations found that 70% of these organizations integrated three or more tools and that 40 percent integrated four or more tools in their toolchains (Kersten, 2018). The same survey also found that a number of software vendors have been emerging recently to provide tools to support the DevSecOps environment. While high automation has been effective in improving DevOps capabilities, some experts argue that assessing and testing security can be difficult to automate (Mansfield-Devine, 2018). For this reason, the successful transition to DevSecOps goes beyond implementing security into the DevOps toolchain by emphasising the human talent. To build an information security culture, organizations also need to address behavioural changes within the development team and the operations team (Mansfield-Devine, 2018). Integrating the security team with the development teams and operations teams to work in collaboration as an effective cross-functional team and ensuring that security is included in every stage of the software development lifecycle can be a formidable challenge.

Trends outside organizational boundaries also present a formidable challenge. According to IBM (2021), the average global cost of a data breach now exceeds $4 million. Despite increasing regulation by the EU General Data Protection Regulation (GDPR) and the European Union Agency for Network and Information Security (ENISA), the increasing trend towards developing cloud-based services and applications using agile development processes also presents major security concerns (Kumar and Goyal, 2020). The COVID-19 global pandemic that has given impetus for executing work-from-anywhere using critical software applications is adding to these security vulnerabilities (Naidoo, 2020). The same IBM report found that the average cost of breaches was $1.07 million higher in organizations supporting remote work.

Markets and Markets (2021) predicts that DevSecOps will grow at a compound annual growth rate of 31.2% reaching $5.9b in 2023. Since DevSecOps is a fairly new trend, the many challenges facing DevSecOps work practices have not been sufficiently addressed in the emerging DevSecOps literature. The review presented in this paper attempts to address these concerns by applying a sociotechnical systems (STS) approach as a framework to provide a more holistic analysis of the social and the technical challenges facing current DevSecOps practices. In addition, this review aims to provide researchers with gaps in current research.

The rest of the paper is organized as follows: first, we outline the socio-technical work system (STWS) framework as a basis for our analysis. Second, we present our systematic literature approach to review the selected DevSecOps literature in more detail. We then present and discuss the results. Finally, we draw theoretical and practical implications for the future of DevSecOps before concluding the paper.

2. Conceptual foundations

We conceive DevSecOps to be a socio-technical work system (STWS). According to Alter (2013), a work system can be defined as “a system in which human participants and/or machines perform work (processes and activities) using information, technology, and other resources to produce specific products/services for specific internal and/or external customers.” A socio-technical lens considers both the social and technical sub-systems of a work system (Sarker et al, 2019). The social sub-system is people oriented and focuses on individuals, their relationships, reward systems and authority structures (Bostrom and Heinen, 1977). The technical sub-system includes tasks, processes and technologies for achieving objectives or outcomes (Bostrom and Heinen, 1977). In a STWS, the fit between the social and the technological subsystems determines the effectiveness of the work system (Sarker et al, 2019). This requires the joint optimisation of both systems in improvement efforts. Improving the performance of STWS have instrumental and humanistic outcomes or objectives. Instrumental objectives are concerned with achieving economic objectives whereas the humanistic objectives are concerned with enhanced job satisfaction and higher quality of working life (Bostrom and Heinen, 1977). Figure 1 depicts the socio-technical work system model which will be used as an initial sensitising framework to assess how researchers are studying DevSecOps.

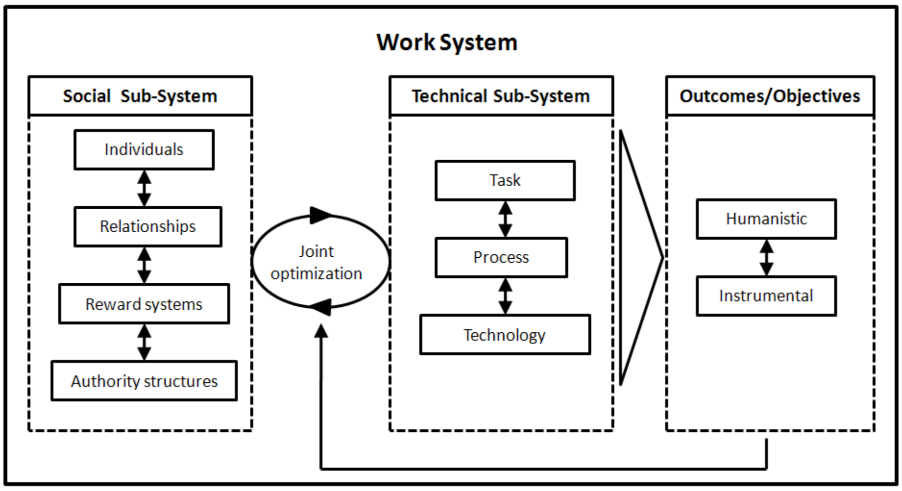

Figure 1: DevSecOps as a Socio-Technical Work System (adapted from Bostrom and Heinen, 1977; Sarker et al, 2019)

Figure 2 shows how Sarker et al. (2019) uses six types to characterise how IT researchers study the socio-technical perspective and its influence on outcomes/objectives: Type I studies are *predominantly social* and focus mainly on how human factors explain outcomes in technology-mediated work systems. Type II or *social imperative* studies consider how social aspects influence the technical component and outcomes. Type III studies consider how *social-technical factors additively deliver outcomes*. These studies assume that there is no interplay between technical and social components. Type IV studies consider how the *socio-technical interplay delivers outcomes*. Type V or *technical Imperative* studies assume that technology is a significant antecedent to social outcomes. Type VI studies are *predominantly technical* and focuses on how to develop or improve the technical component of a work system with little or no consideration of the social component. The STWS lens and these six types are appropriate for analysing the DevSecOps literature as research should strive to provide a balanced focus on both the social and the technical subsystems and the optimal interaction between these subsystems so that organizations achieve both their humanistic and instrumental objectives of DevSecOps. The purpose of this paper is to understand to what extent the literature considers the interplay of the social and technical within a DevSecOps work system in delivering outcomes or objectives.

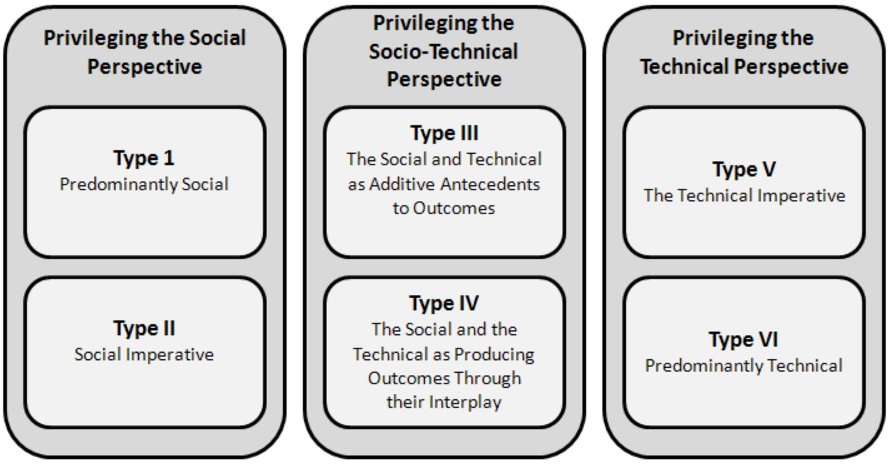
Privileging the Social Perspective
Type 1
Predominantly Social
Type II
Social Imperative
Privileging the Socio-Technical Perspective
Type III
The Social and Technical as Additive Antecedents to Outcomes
Type IV
The Social and the Technical as Producing Outcomes Through their Interplay
Privileging the Technical Perspective
Type V
The Technical Imperative
Type VI
Predominantly Technical

Figure 2: Types of socio-technical research (adapted from Sarker et al, 2019)

3. Research method

We conducted a systematic literature review on DevSecOps. Our inclusion criteria were as follows: The article contents should be about implementing DevOps and focus on security. Based on a preliminary analysis, our final search string was composed as follows: ("DevOps" OR "DevSecOps") AND ("security" OR "secur*" OR “cybersecur*”) AND ("applications" OR "software") AND ("develop*" OR "build"). We search the following databases using the defined search strings: ScienceDirect, IEEE Xplore, and ABI/INFORM Collection. We filtered the source types to include journals only. Furthermore, we considered only English publications. 141 one articles were eligible for further analysis.

We applied the following filtering process to select the relevant literature. First, articles were identified by using our defined search string. Next, we removed duplicate articles from the source list. The remaining articles were then screened, by reading the abstract of each article. After reading the abstracts, articles that did not support the research question were excluded from the source list. Finally, the screened sources were assessed for eligibility by reading the entire article. Table 1 shows the results achieved in each step.

Table 1: Results of the filtering process

Filter process steps	Results
Identify articles	141
Remove duplicates	123
Screen abstract	60
Screen full text	28

To ensure that the article was relevant, quality assessment criteria in the form of questions were created to determine if security themes in a DevOps or similar environment was adequately discussed. One of the authors engaged in member checking to check the accuracy of the filtering process and plausibility of the thematic analysis (Yin, 2014). Table 2 depicts details of journal publications. The majority of articles are from technically oriented disciplines such as software engineering, network security, computer science and computer security.

Table 2: Journal publication details

Journal	No. of papers
IEEE Software	12
Network Security	5
IEEE Internet Computing	2
Journal of Management Information and Decision Sciences	1
Computer	1
Computer Fraud & Security	1
IET Software	1
Computers & Security	1
Journal of Systems and Software	1
Computing in Science & Engineering	1
AI & Society	1
IEEE Access	1

4. Results

We draw on the socio-technical work system framework for DevSecOps (see Figure 1) to present our results. The framework includes three practice categories and 11 practice dimensions. Figure 3 presents the six types of socio-technical perspectives and their influence on social and instrumental outcomes/objectives. Table 3 provides a condensed overview of how the framework can be used to assess the challenges facing organizations in jointly optimising their DevSecOps work system. Figure 3 shows Type VI, which refers to predominantly technical studies that lacks the consideration of humanistic outcomes, and Type III, which focuses on how social-technical factors additively deliver outcomes, were the two dominant perspectives adopted by DevSecOps researchers.

The majority of Type VI studies were focused on how to improve tasks, processes and technologies to improve the instrumental outcomes as a measure of DevSecOps performance (McGraw, 2017; Casola et al, 2020; Almuairfi and Alenezi, 2020; Kersten, 2018). Within these group of studies, references were made to security policies, threat modelling and risk assessment processes, tasks such as code reviews, application security testing, static analysis, software composition analysis and dynamic analysis, dynamic application security testing (DAST), interactive application security testing, penetration testing, and technologies such as software containers, secure cloud applications and security tools.

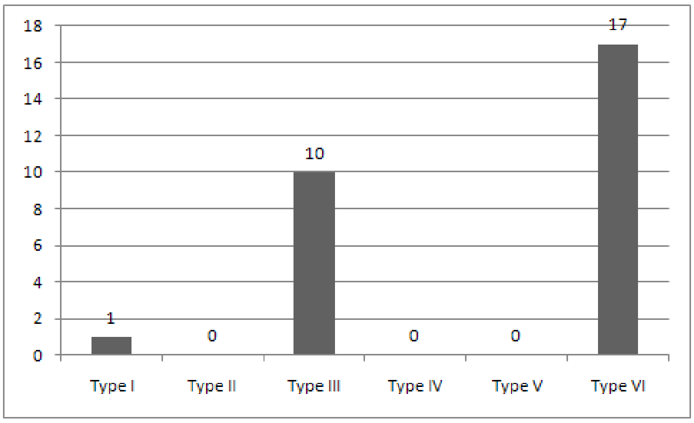

Figure 3: Number of DevSecOps studies by Types of Socio-technical Research

There was only one study for Type I where behavioural factors of developers, operators and security staff were seen to explicitly influence the outcome of the DevSecOps work system (Carter, 2017). This predominantly social study highlighted the importance of culture, inclusion, knowledge sharing, teamwork, and security training in developing a high-performance security team. A number of studies appear to belong to Type III and focused on how social and technical factors additively deliver outcomes (Bass, 2018; Mansfield-Devine, 2018; Tufin, 2020). We grouped our analysis of the social sub-system practice category by individuals, relationships, reward systems, and authority structures. The literature focuses on social actors such as individuals (Operators, Developers, Security Champion, Security Experts, End Users, Product Owners, and Project Managers) and teams (Operations teams, DevOps Teams, Security Teams). This literature also emphasises the importance of collaboration, communication and feedback between the Security team and DevOps teams in realizing continuous security. Apart from teamwork, the knowledge, skills, attitudes and behaviour of individuals and teams were highlighted (Bass, 2018; Mansfield-Devine, 2018; Tufin, 2020).

We found no study that viewed DevSecOps as explicitly consisting of two sub-systems, DevSecOps processes to achieve joint optimisation of these sub-systems, and the socio-technical interplay that generates the outcomes for the entire DevSecOps work system. Our analysis also did not reveal any Type II or social imperative studies. This is not surprising given the role of technology in achieving positive outcomes in complex DevSecOps environments. Surprisingly, there were no Type V or technical Imperative studies which focused solely on technology and its influence in achieving humanistic outcomes.

Table 3: Selected themes from the literature

Practice Category	Practice Dimensions	Themes
Social Sub-System	Individuals	The social impact of the changing work roles of developers, operators, security experts and end-users.
		The evolving security threats posed by external and internal actors.
	Relationships	The challenge of developing a collaborative cross-functional team that communicates effectively.
	Reward Systems	The challenge of aligning incentives to overall goals (safe and secure software) that conflicts with local goals (speed versus stability).
	Authority Structures	Escalating potential security threats to the product manager or business representatives.
Technical Sub-System	Tasks	Performing application security testing using code reviews, static analysis, software composition analysis, dynamic analysis and penetration testing.
	Process	The use of threat modelling to inform the risk assessment process.
	Technology	Full or Semi-Automation using Dynamic Application Security Testing (DAST) or Interactive Application Security Testing (IAST) tools.
Outcomes/Objectives	Humanistic (Positive)	The benefits of job enrichment and job enlargement
		The downside of job enlargement

Practice Category	Practice Dimensions	Themes
	Humanistic (Negative)	Teams at loggerheads (e.g. developer resistance).
	Instrumental (Positive)	Security issues are identified and fixed much earlier in the lifecycle.
		Implementing security requirements using automation to reduce delays.
		Agility and velocity in delivering time-to-market applications and services in a cost-effective manner.
	Instrumental (Negative)	Time consuming and resource intensive security activities slow down the pipeline.
		The cost of security breaches.

5. Discussion

Our results suggest that studying the interplay of the social and technical within a DevSecOps work system in delivering both instrumental and humanistic outcomes and objectives is an understudied area. Given that the majority of review articles were from technically oriented disciplines such as systems engineering, computer science and computer security, it is not surprising that these articles' focus was predominantly technical. However, many of these articles did acknowledge the importance of social factors to varying degrees. Our study suggest three important avenues for future research: First, this study complements prior work on socio-technical work systems by specifying the sub-systems, dimensions, challenges and outcomes that are more salient in the DevSecOps work system (Bostrom and Heinen, 1977; Alter, 2013; Sarker et al, 2019). Our study goes beyond prior research in DevOps and DevSecOps that emphasise people, process and technology factors by specifying a richer set of interacting elements in socio-technical work systems (Kumar and Goyal, 2020). It would be interesting to see future research studies focusing on a richer set of socio-technical concepts especially in organizational contexts where the socio-technical may interplay. Second, we infer from our analysis that DevSecOps may raise concerns about the impact of technology on the social sub-systems. For example, workers may be concerned that automation technologies will be used to replace staff. These types of social impacts have been under researched. Third, many of the studies considered DevSecOps as a vehicle to achieve instrumental objectives/outcomes without considering the social outcome, that is, how new work role transitions in DevSecOps influences job satisfaction and employee well-being. Instead, instrumental outcomes such as reducing time to market delays and cost-effectiveness were emphasized. Further studies should emphasize social outcomes at the outset for two reasons. Firstly, a socio-technical perspective strives to humanise the DevSecOps work environment which can be beneficial when teams are at loggerheads or individuals resist the change to DevSecOps. Secondly, the social dimension can improve DevSecOps performance, which has not been explicitly studied by the articles in this review.

Viewing and analysing DevSecOps using a socio-technical work system framework offers the following specific questions that could be promising for future research:

1. How do systems outside the organizational boundary influence DevSecOps work practices?
2. How do successful DevSecOps environment manage individual and/or team resistance to change?
3. What interventions are used to align the technical and social environments?
4. To what extent does organizational culture constrain and enable DevSecOps work practices?
5. To what extent does work role changes in transitioning to DevSecOps result in role-related stress?
6. How can the interplay between technology and human activities improve the performance of DevSecOps?

A sociotechnical perspective also offers new possibilities for refining prior models on cyber warfare and security that tend to be either sociocentric or technocentric (Sánchez-Gordón and Colomo-Palacios, 2020; Fletcher and Smith, 2020; Huskaj, 2019). The proposed socio-technical model offers an analytical approach that focuses on the interplay between technology and human activities, arguably providing more balanced insights about cyber challenges in domains such as cyber conflict, cyber terrorism, cyber security and information warfare (Izycki and Wallier, 2021; Huskaj, 2019). A socio-technical perspective is also salient to conceptualizing key cyber challenges. For example, by drawing attention to the interactions between the social and the technological subsystems a socio-technical perspective can offer a novel conceptualization of cyber resilience (Fletcher and Smith, 2020).

Pedagogic practices in cyber warfare and security vocational training and education can also benefit from understanding the entwined nature of social and technological relations (Avis, 2018).

Our study has four main limitations. First, our literature review might not be exhaustive due to the composition of our search string. Second, we limited our search to three databases. Therefore, the articles not found in these databases were excluded in this review. Third, in order to meet all inclusion criteria, a number of articles were filtered out manually by screening the abstract and the article. Despite member checking, our final set of articles could be prone to selection bias. Fourth, although we argue that our proposed socio-technical framework is a useful sensitising tool for further research and in practice for assessing the state of DevSecOps in organizations, our depiction and understanding of the socio-technical dimensions may lack completeness and it is also plausible that either the social or technical may be irrelevant in certain DevSecOps contexts.

6. Conclusion

Based on a systematic literature review, we found that technical studies that pay little consideration to humanistic outcomes feature prominently in the literature. Based on our coding process and thematic analysis, we developed a framework to improve our understanding of DevSecOps based on the insights from the reviewed articles using a socio-technical lens. The socio-technical framework can be used by practitioners to perform a more holistic analysis of their DevSecOps practices for realizing continuous security. It highlights the key social and technical themes that underpin the effectiveness of DevSecOps and how insights about these themes can be used by practitioners to improve the instrumental and humanistic goals of DevSecOps. An interdisciplinary approach is proposed to adequately address challenging socio-technical relationships in DevSecOps. Drawing from the socio-technical work system framework and insights from the literature, we identified avenues for future research that address social imperatives as well as humanistic objectives and outcomes. Future research can empirically test the importance of the interplay between technology and human activities to improve the overall performance of DevSecOps.

7. References

Almuairfi, S. and Alenezi, M. (2020) "Security controls in infrastructure as code", *Computer Fraud & Security*, Vol 2020 No. 10, pp 13–19.

Alter, S. (2013) "Work system theory: overview of core concepts, extensions, and challenges for the future", Journal of the Association for Information Systems, Vol 14, No. 2, pp 72–121.

Amoroso, E. (2018) "Recent Progress in Software Security", *IEEE Software*, Vol 35, No. 2, pp 11–13.

Anderson, C. (2015) "Docker [Software engineering]", *IEEE Software*, Vol 32, No. 3, pp 102–c103.

Atwood, C. A., Goebbert, R. C., Calahan, J. A., T. V. Hromadka, I., Proue, T. M., Monceaux, W. and Hirata, J. (2016) "Secure Web-Based Access for Productive Supercomputing", *Computing in Science & Engineering*, Vol 18, No. 1, pp 63–72.

Avis, James. (2018) "Socio-technical imaginary of the fourth industrial revolution and its implications for vocational education and training: A literature review." Journal of Vocational Education & Training, Vol 70, No. 3, pp 337–363.

Bass, L. (2018) "The Software Architect and DevOps", *IEEE Software*, Vol 35, No. 1, pp 8–10.

Bostrom, R. P. and Heinen, J. S. (1977) "MIS problems and failures: A socio-technical perspective. Part I: The causes", MIS quarterly, pp 17–32.

Callanan, M. and Spillane, A. (2016) "DevOps: Making It Easy to Do the Right Thing", *IEEE Software*, Vol 33, No. 3, pp 53–59.

Carter, K. (2017) "Francois Raynaud on DevSecOps", *IEEE Software*, Vol 34, No. 5, pp 93–96.

Casola, V., De Benedictis, A., Rak, M. and Villano, U. (2020) "A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach", *Journal of Systems and Software*, Vol 163, pp 110537.

Clarke, V. and Braun, V. (2017) "Thematic analysis", *The Journal of Positive Psychology*, Vol 12, No. 3, pp 297–298.

Cope, R. (2020) "Strong security starts with software development", *Network Security*, Vol 2020, No. 7, pp 6–9.

Dyess, C. (2020) "Maintaining a balance between agility and security in the cloud", *Network Security*, Vol 12, No. 3, pp 14–17.

Ebert, C., Gallardo, G., Hernantes, J. and Serrano, N. (2016) "DevOps", *IEEE Software*, Vol. 33, No. 3, pp 94–100.

Fletcher, K. and Smith, H. A. (2020) "Cyber Resilience through Machine Learning: Data Exfiltration" In International Conference on Cyber Warfare and Security, pp. 165-XIII. Academic Conferences International Limited, 2020.

Gatrell, M. (2016) "The Value of a Single Solution for End-to-End ALM Tool Support", *IEEE Software*, Vol 33, No. 5, pp 103–105.

Huskaj, G. (2019) "The Current State of Research in Offensive Cyberspace Operations" In European Conference on Cyber Warfare and Security, pp. 660–XIV. Academic Conferences International Limited.

IBM (2021) "Cost of Data Breach Report", [online], https://www.ibm.com/security/databreach (accessed on 12 January 2021).

Izycki, E. and Vianna, E. W. "Critical Infrastructure: A Battlefield for Cyber Warfare?" In ICCWS 2021 16th International Conference on Cyber Warfare and Security, pp. 454. Academic Conferences Limited, 2021.

Jansen, C. and Jeschke, S. (2018) "Mitigating risks of digitalization through managed industrial security services", *AI & Society*, Vol 33, No. 2, pp 163–173.

Johann, S. (2017) "Kief Morris on Infrastructure as Code", *IEEE Software*, Vol 34, No. 1, pp 117–120.

Kersten, M. (2017) "Value Stream Architecture", *IEEE Software*, Vol 34, No. 5, pp 10–12.

Kersten, M. (2018) "A Cambrian Explosion of DevOps Tools", *IEEE Software*, Vol 35, No. 2, pp 14–17.

Klein, D. (2019) "Micro-segmentation: securing complex cloud environments", *Network Security*, Vol 2019, No. 3, pp 6–10.

Kumar, R. and Goyal, R. (2020) "Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC)", *Computers & Security*, Vol. 97, pp 101967.

MacDonald, N., (2012) "Devops needs to become devopssec", [online], https://blogs.gartner.com/neil_macdonald/2012/01/17/devops-needs-to-become-devopssec/ (accessed on 09 November 2015).

Mackey, T. (2018) "Building open source security into agile application builds", *Network Security*, Vol 2018, No. 4, pp 5–8.

Mansfield-Devine, S. (2018) "DevOps: finding room for security", *Network Security*, Vol 2018, No. 7, pp 15–20.

Markets and Markets, (2021) "Devsecops market", [online], https://www.marketsandmarkets.com/PressReleases/devsecops.asp. (accessed on 12 January 2021).

McGraw, G. (2017) "Six Tech Trends Impacting Software Security", *Computer*, Vol 50, No. 5, pp 100–102.

Mohan, V. and Othmane, L. B. (2016) "Secdevops: Is it a marketing buzzword?-mapping research on security in devops" In 2016 11th international conference on availability, reliability and security (ARES), pp. 542-547. IEEE.

Myrbakken, H., and Colomo-Palacios, R. (2017) "DevSecOps: a multivocal literature review" In International Conference on Software Process Improvement and Capability Determination, pp. 17-29. Springer, Cham.

Naidoo, R. (2020) "A multi-level influence model of COVID-19 themed cybercrime", European Journal of Information Systems, Vol 29, No. 3, pp 306–321.

Parnin, C., Helms, E., Atlee, C., Boughton, H., Ghattas, M., Glover, A., Holman, J., Micco, J., Murphy, B., Savor, T., Stumm, M., Whitaker, S. and Williams, L. (2017) "The Top 10 Adages in Continuous Deployment", *IEEE Software*, Vol 34, No. 3, pp 86–95.

Rafi, S., Yu, W., Akbar, M. A., Alsanad, A. and Gumaei, A. (2020) "Prioritization Based Taxonomy of DevOps Security Challenges Using PROMETHEE", *IEEE Access*, Vol 8, pp 105426–105446.

Rahman, A. A. U., and Williams, L. (2016) "Software security in devops: Synthesizing practitioners’ perceptions and practices" In *2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED),* pp. 70-76. IEEE.

Rios, E., Iturbe, E., Larrucea, X., Rak, M., Mallouli, W., Dominiak, J., Muntés, V., Matthews, P. and Gonzalez, L. (2019) "Service level agreement-based GDPR compliance and security assurance in(multi)Cloud-based systems", *IET Software*, Vol 13, No. 3, pp 213–222.

Sánchez-Gordón, M. and Colomo-Palacios, R. "Security as culture: a systematic literature review of DevSecOps." In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pp. 266-269. IEEE/ACM.

Sarker, S., Chatterjee, S., Xiao, X. and Elbanna, A. (2019) "The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance", *MIS Quarterly*, Vol 43, No. 3, pp 695–720.

Spinellis, D. (2012) "Don't Install Software by Hand", *IEEE Software*, Vol 29, No. 4, pp 86–87.

Trihinas, D., Tryfonos, A., Dikaiakos, M. D. and Pallis, G. (2018) "DevOps as a Service: Pushing the Boundaries of Microservice Adoption", *IEEE Internet Computing*, Vol 22, No. 3, pp 65–71.

van Dinter, R., Tekinerdogan, B. and Catal, C. (2021) "Automation of systematic literature reviews: A systematic literature review", *Information and Software Technology*, Vol 136, pp 106589.

Weber, I., Nepal, S. and Zhu, L. (2016) "Developing Dependable and Secure Cloud Applications", *IEEE Internet Computing*, Vol 20, No. 3, pp 74–79.

Winter, S., Berente, N., Howison, J. and Butler, B. (2014) "Beyond the organizational ‘container’: Conceptualizing 21st century sociotechnical work", *Information and Organization*, Vol 24, No. 4, pp 250–269.

Yin, R. K. (2014) *Case study research: Design and methods (5th ed.)*, Sage, California.

Zaydi, M. and Nassereddine, B. (2020) "DevSecOps Practices for an Agile and Secure IT Service Management", *Journal of Management Information and Decision Sciences*, Vol 23, No. 2, pp 1–16.