IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46SP/2025/4630325/
Vol. 2025 (37), Article ID 4630325

The Role of DevSecOps in Ensuring Business Continuity and Resiliency of GIS Systems*

Maciej KIEDROWICZ, Jerzy STANIK and Kazimierz WORWA

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Maciej KIEDROWICZ, maciej.kiedrowicz@wat.edu.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

This article explores the integration of security practices within the DevSecOps methodology in the context of Geographic Information Systems (GIS). The primary objective of the study is to analyze the impact of DevSecOps on ensuring business continuity and system resilience against cybersecurity threats. The specific goals of the research include:

- evaluating the effectiveness of DevSecOps in enhancing the resilience of GIS systems,
- identifying the benefits of automating security processes throughout the software development lifecycle (SDLC),
- analyzing organizational and technical challenges associated with implementing DevSecOps across various sectors.

The novelty of the study lies in applying DevSecOps to the GIS domain, which is characterized by high demands for data availability, spatial data integrity, and regulatory compliance. The authors argue that traditional security approaches, typically implemented at the end of the system lifecycle, are insufficient in the face of evolving cyber threats. The article presents empirical findings and case studies from multiple organizations, demonstrating the practical benefits of DevSecOps in GIS environments. These include faster detection and remediation of vulnerabilities, increased automation of security testing, and improved system resilience. The study contributes to the growing body of knowledge on GIS security and offers practical recommendations for organizations adopting DevSecOps
.

Keywords: DevSecOps, GIS, business continuity, system resilience, automation, cybersecurity

Introduction

Modern Geographic Information Systems (GIS) operate in a dynamic digital environment where increasing cybersecurity threats and demands for operational continuity pose significant challenges to organizations. Traditional security models, often implemented at the final stages of the software lifecycle, are insufficient for systems requiring high availability, spatial data integrity, and regulatory compliance.

Cite this Article as: Maciej KIEDROWICZ, Jerzy STANIK and Kazimierz WORWA, Vol. 2025 (37) "The Role of DevSecOps in Ensuring Business Continuity and Resiliency of GIS Systems " Communications of International Proceedings, Vol. 2025 (37), Article ID 4630325, https://doi.org/10.5171/2025.4630325

DevSecOps, an evolution of DevOps that integrates security practices throughout the software development lifecycle (SDLC), offers an initiative-taking approach to risk management through automation, continuous monitoring, and early vulnerability detection. In the context of GIS, DevSecOps can significantly enhance system resilience and reduce operational downtime.
Despite growing interest in DevSecOps, the academic literature still lacks empirical studies focused on its application in GIS environments, particularly within public sector and academic institutions. This article investigates the impact of DevSecOps on the continuity and resilience of GIS systems.

The main objectives of the study are:

- To evaluate the effectiveness of DevSecOps in managing security incidents within GIS systems.
- To identify the benefits of automating security processes across the GIS software lifecycle.
- To analyze organizational and technical challenges associated with DevSecOps implementation in various sectors.

The article is structured into five sections: introduction, literature review, research methodology, results and discussion, and conclusions with practical recommendations.

Literature Review

Existing Research and DevSecOps Approaches

DevSecOps is increasingly recognized as a key methodology for building resilient IT systems. Sandu (2021) emphasizes that embedding security early in the DevOps lifecycle is essential for achieving resilience, especially in distributed GIS environments. Smith and Brown (2022) describe it as a model that integrates security throughout the software lifecycle, though their work does not address the unique requirements of GIS systems, such as spatial data availability and cross-platform interoperability.

Prates and Pereira (2024) conducted a multivocal literature review identifying core DevSecOps practices and tools. While they emphasize automation and security integration, their study lacks specific insights into GIS applications and regulatory constraints such as GDPR and the NIS2 directive.

Rodriguez et al. (2024) proposed a DevSecOps maturity model that correlates security integration with deployment frequency and incident response time. This model is particularly relevant for GIS systems deployed in high-availability environments.

Fu, Pasuksmit, and Tantithamthavorn (2024) explored the role of artificial intelligence in DevSecOps, highlighting its potential to automate security testing, anomaly detection, and real-time incident response—capabilities crucial for GIS platforms that process continuous data streams.

In the public sector, the U.S. Department of Defense (DoD, 2025) reported over 50 software factories implementing DevSecOps in high-risk environments. These initiatives have led to shorter deployment cycles, improved code quality, and enhanced system resilience. Veeramachaneni (2023) confirms that DevSecOps practices contribute to bridging agile development and security, enhancing deployment speed and reducing vulnerabilities.

Identified Research Gaps

Despite the growing body of literature, several gaps remain in the study of DevSecOps within GIS contexts:

- **Lack of empirical studies**: Most publications are conceptual or technical, with limited evidence from real-world GIS deployments (Cybersecurity Ventures, 2024; Prates & Pereira, 2024).
- **Absence of case studies**: There is a shortage of documented DevSecOps implementations in GIS, particularly regarding incident response and ransomware protection (Synopsys, 2023; IBIMA, 2025).
- **Organizational adaptation**: DevSecOps adoption in public institutions requires alignment with formal procedures, legal frameworks, and budgetary constraints (DoD, 2025; GitLab, 2024).

- **Cultural factors**: Few studies examine how organizational culture affects DevSecOps success in interdisciplinary and geographically distributed GIS teams (GovCIO, 2025).
- **Automation of traditional security practices**: Research tends to focus on novel techniques, overlooking the automation of essential practices such as access control and data backup (Abdiukov, 2024).

Methodology

Research Objective

The objective of this study is to examine how the implementation of DevSecOps practices influences the continuity and resilience of Geographic Information Systems (GIS). The research aims to provide empirical evidence on the effectiveness of DevSecOps in improving security response times, reducing system downtime, and enhancing organizational preparedness against cyber threats.

Research Design

A **mixed-methods approach** was adopted, combining qualitative and quantitative techniques to ensure a comprehensive understanding of DevSecOps in GIS environments. The conceptual framework proposed by Gbenle et al. (2025) was used to guide the integration of secure deployment and CI/CD practices in the research design. The study was conducted in two phases:

- **Phase I – Literature Review**: A systematic review of existing academic and industry publications was performed to identify theoretical foundations, current practices, and research gaps.
- **Phase II – Empirical Study**: Data were collected from five organizations across different sectors (technology, healthcare, education, manufacturing, and public administration) that have implemented DevSecOps in GIS-related systems.

Data Collection Methods

To ensure a comprehensive understanding of current DevSecOps practices in GIS environments, a mixed-methods approach was adopted. As shown in Table 1, data collection involved stakeholder interviews, case study analysis, survey research, document analysis, and expert interviews. Each method was supported by appropriate tools, such as Firmbee for stakeholder interviews and Microsoft Power BI for case study analysis, enabling both qualitative and quantitative insights into the integration of security within DevOps pipelines.

Table 1. Data Collection Methods

Method	Description	Tool Used
Stakeholder Interviews	Semi-structured interviews with GIS managers, DevOps engineers, and security specialists.	Firmbee
Case Study Analysis	In-depth examination of DevSecOps implementations in five organizations.	Microsoft Power BI
Survey Research	Online questionnaires distributed to GIS professionals to collect quantitative data on DevSecOps practices.	Google Forms
Document Analysis	Review of technical documentation, audit reports, and security logs from participating organizations.	MAXQDA

Expert Interviews	Interviews with subject-matter experts to gather insights on best practices and future trends.	Transcription tools

Sampling and Participants

The study involved five organizations selected based on their active use of GIS systems and adoption of DevSecOps practices. Participants included technical staff, security officers, and decision-makers involved in system development and maintenance.

Data Analysis

Quantitative data from surveys and case studies were analyzed using descriptive statistics and comparative metrics (e.g., MTTD, MTTR, deployment frequency). Qualitative data from interviews and document analysis were coded and thematically analyzed to identify recurring patterns and challenges.

Limitations

Several limitations should be considered when interpreting the results:

- **Sample Size**: The study includes a limited number of organizations, which may affect generalizability.
- **Self-Reporting Bias**: Survey and interview responses may be influenced by subjective perceptions.
- **Data Availability**: Not all organizations were able to provide complete documentation, which may limit the depth of analysis.

Results and discussion

The structure of this chapter is as follows:

1. Presentation of results – a detailed presentation of the results obtained and graphs, tables and other visualizations of data that help in understanding the results.
2. Analysis of results – interpretation of results in the context of research objectives and comparison of results with previous research and literature on the subject.
3. Discussion – discussion of the importance of the results and their practical implications, analysis of potential limitations of the study and their impact on the results, and proposals for further research and directions of development in this field.
4. Case studies showing how DevSecOps has contributed to the resilience of systems to threats.

Presentation of results

The study analysed the impact of DevSecOps implementation on the continuity and resilience of IT systems in 5 organizations from different sectors: Company A – technology company, Company B – University Hospital, Company C – University of Technology, Company D – medium-sized manufacturing company, Company E – university.

The results of the research are presented in the form of tables and line graphs divided into two groups:

- key security indicators highlighting the role of DevSecOps in ensuring business continuity and resiliency of systems
- additional metrics that are useful in the context of DevSecOps.

In addition, this chapter characterizes key tools that can help you monitor metrics related to business continuity and resiliency of systems.

Presentation of results for key security measures

Table 2 illustrates key security indicators that highlight the role of DevSecOps in ensuring business continuity and resiliency of systems.

Table.2. Specification of key measures to ensure business continuity and resilience of systems

Gauge	Specification
Time to Detect and Repair (MTTD/MTTR)	The speed at which your team is able to detect and fix vulnerabilities is critical to minimizing risk and ensuring business continuity
Number of security incidents	Monitoring the number of security incidents before and after implementing DevSecOps practices can show the effectiveness of these practices in mitigating threats
Deployment frequency	This metric measures how often new software releases are deployed. Higher deployment frequency means more automated and secure processes
Mean Time to Recovery (MTTR)	It measures the time it takes to restore the system to full functionality after a failure. Reduced downtime to increase system resiliency
Security Test Automation Percentage	This indicator shows how much of the security testing is automated. A higher level of automation means faster and more effective problem detection.

Table 3 provides empirical data collected through observations, experiments, or experiences from five companies that are designed to illustrate the potential benefits of implementing DevSecOps practices.

Table 3. Data for five companies, including before and after DevSecOps

COMPANY / **Indicator**	Company A (formerly)	Company A (after)	Company B (formerly)	Company B (after)	Company C (formerly)	Company C (after)	Company D (Formerly)	Company D (after)	Company E (formerly)	Signature E (BR)
Time to Detect (MTTD) [days]	7	2	10	3	8	2	12	4	9	3
Time to Fix a Vulnerability (MTTR)[days]	14	5	20	7	15	6	18	8	16	6
Number of security incidents	15	5	20	7	18	6	22	8	19	6
Deployment frequency [week]	4	1	4	2	4	1	4	2	5	1

COMPANY / Indicator	Company A (formerly)	Company A (after)	Company B (formerly)	Company B (after)	Company C (formerly)	Company C (after)	Company D (Formerly)	Company D (after)	Company E (formerly)	Signature E (BR)
Mean Downtime (MTTR)[hour]	8	2	10	3	9	2	12	4	11	3
Test Automation Percentage [%]	30	80	25	75	35	85	20	70	28	78

Line charts based on this data are shown in Figure 1.

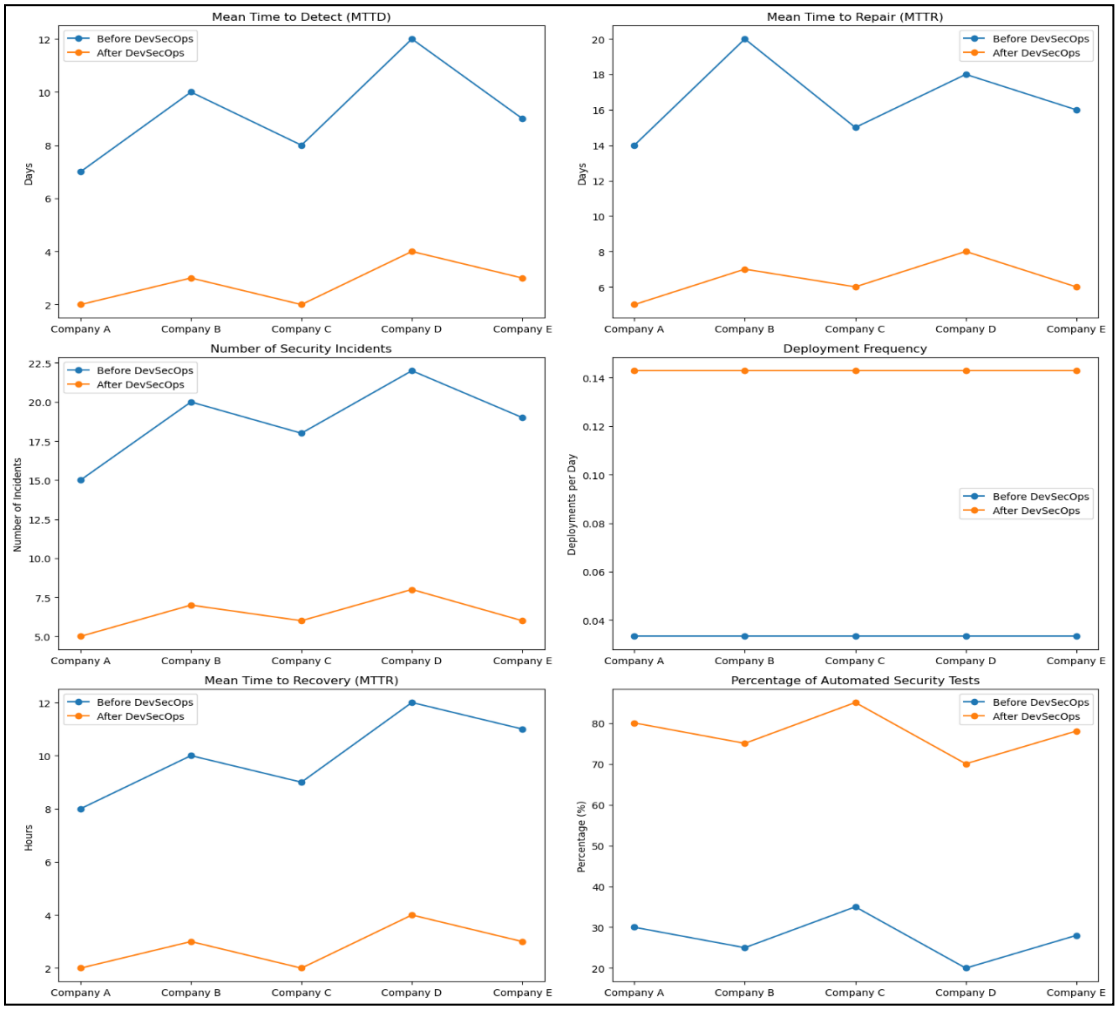

Fig.1. Linear diagrams for key safety indicators

The interpretation of the line charts showing data for the five companies before and after the introduction of DevSecOps practices is as follows:

1. The introduction of DevSecOps has significantly accelerated vulnerability detection, allowing for faster response to threats:
    - Before DevSecOps: Companies took 7 to 12 days to detect vulnerabilities,
    - After DevSecOps: This time has been reduced to 2-4 days.
2. DevSecOps has enabled faster remediation of vulnerabilities, which reduces the risk of long-term threats:
    - Before DevSecOps: Companies took 14 to 20 days to fix vulnerabilities,
    - After DevSecOps: This time has been reduced to 5-8 days.
3. The implementation of DevSecOps has reduced the number of security incidents, indicating an improvement in the overall security posture:
    - Before DevSecOps: Companies had between 15 and 22 security incidents,
    - After DevSecOps: the number of incidents dropped to 5-8.
4. DevSecOps allows for more frequent and automated deployments, which increases flexibility and responsiveness to change:
    - Before DevSecOps: Companies deployed new software releases once a month,
    - After DevSecOps: Deployment frequency increased to once a week or twice every two weeks.
5. DevSecOps improved the resilience of systems by reducing the time it takes to recover from a disaster:
    - Before DevSecOps: Companies had an average downtime of 8 to 12 hours.
    - After DevSecOps: This time has been reduced to 2-4 hours.
6. A higher level of security test automation means faster and more effective problem detection, which increases overall process efficiency:
    - Before DevSecOps: test automation was between 20% and 35%.
    - After DevSecOps: automation increased to 70%-85%.

In conclusion, implementing DevSecOps brings significant benefits in terms of security, business continuity, and system resiliency. Businesses can respond to threats faster, deploy new software releases more frequently, and minimize downtime for better performance and operational stability.

Presentation of results on additional safety measures

A set of additional metrics that are useful in the context of DevSecOps is shown in Table 4.

Table 4. List of indicators related to business continuity

Metric	**Specification**
Scope of safety tests	The percentage of code that is subject to security testing. Indicates the scope of security tests and their effectiveness in identifying potential threats
Number of vulnerabilities	The number of vulnerabilities identified in the development process. Helps you track trends in identifying and remediating vulnerabilities, ensuring that vulnerabilities are remediated quickly
Code review results	The number and severity of security issues discovered during code reviews. Demonstrates the effectiveness of secure coding practices and code analysis tools
Patch management performance	The time it takes to deploy security patches after they're released. Demonstrates an organization's ability to respond quickly to new threats
False positive rate	The percentage of false positives generated by security monitoring systems. Demonstrates the effectiveness of threat detection tools and minimization of unnecessary interventions
User access reviews	Frequency and results of user access reviews to systems. Helps ensure that only authorized users have access to critical resources
Incident severity levels	Classification of security incidents according to their severity. Helps you prioritize corrective actions and allocate resources
Completion of security awareness training	Percentage of employees who have completed safety training. Indicates the level of security awareness in the organization

Table 5 and 6. contain empirical data collected from observations, experiments, or experiences from five companies that aim to illustrate the potential benefits of implementing DevSecOps practices for complementary indicators.

Tab.5. Data for metrics before DevSecOps implementation

Metric / Company	Safety Test Coverage (%)	Number of security Vulnerabilities	Code Overview Determine	Patch management Yield (days)	False positive result Rate (%)	User access Reviews (per year)	Severity of the event Levels (1-5)	Security Awareness Training Completion (%)
Signature A	70	10	5	5	5	2	3	60
Company B	75	12	6	6	6	2	3	65
Company C	80	15	7	7	7	2	3	70
Company D	85	18	8	8	8	2	3	75
Signature E	90	20	9	9	9	2	3	80

Table 6. Data for metrics before DevSecOps implementation

Metric / Company	Safety Test Coverage (%)	Number of security Vulnerabilities	Code Overview Determine	Patch management Yield (days)	False positive result Rate (%)	User access Reviews (per year)	Severity of the event Levels (1-5)	Completion of security awareness training (%)
Signature A	80	8	3	3	3	4	2	70
Company B	85	10	4	4	4	4	2	75
Company C	90	12	5	5	5	4	2	80
Company D	95	15	6	6	6	4	2	85
Signature E	100	18	7	7	7	4	2	90

Linear diagrams prepared on the basis of the data contained in Table 5 and Table 6 are illustrated in Figure 2.

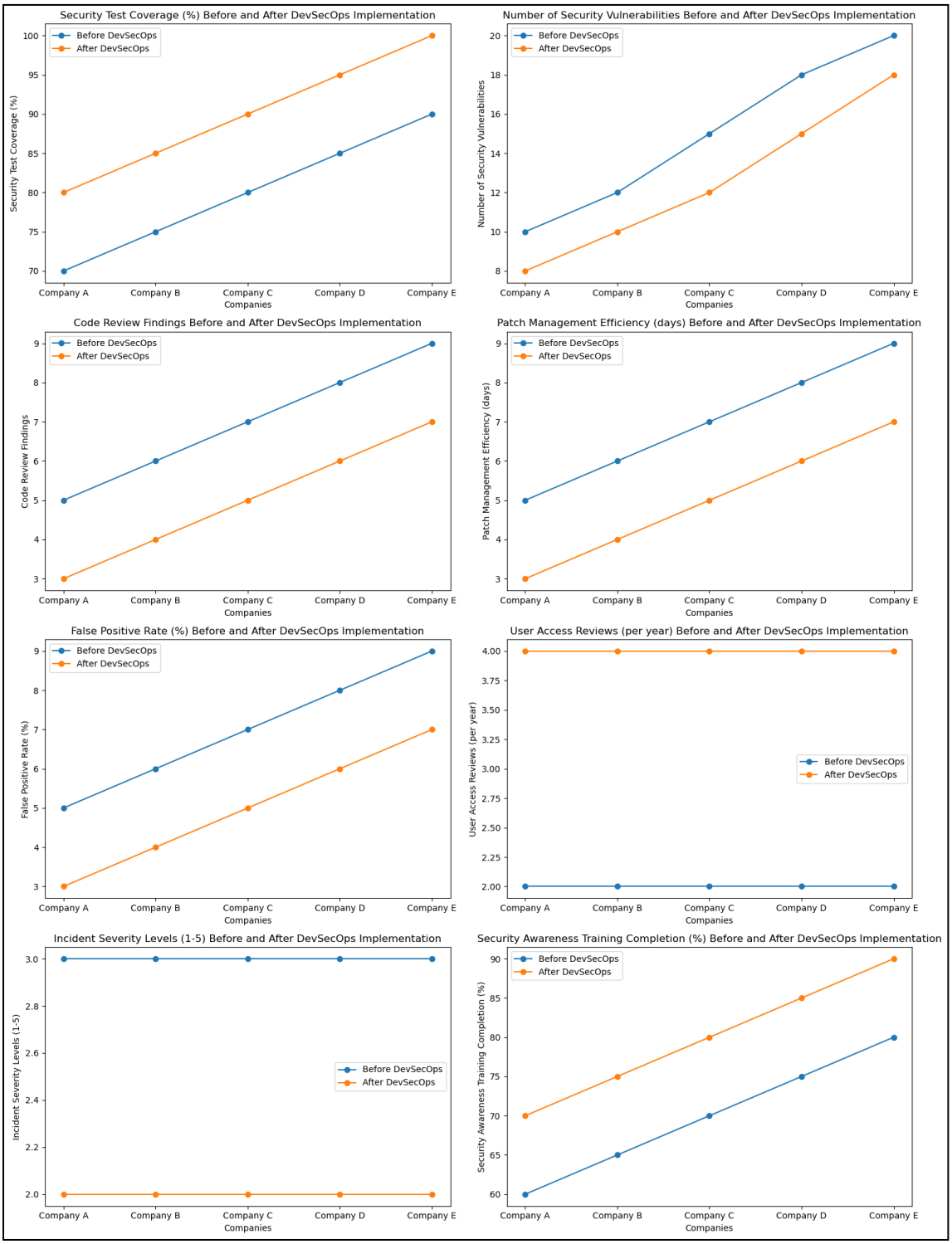

Fig.2. Line charts for business continuity metrics

Based on the charts, we can draw several conclusions about the impact of DevSecOps implementation on business continuity indicators for five companies:

- Increased detection and response efficiency – Reduced detection time (MTTD) and incident remediation (MTTR) means that businesses are able to identify and respond to threats faster, minimizing their impact on systems. This leads to reduced downtime and faster restoration of full functionality.
- Improving the quality and security of coding – Reducing the number of vulnerabilities and issues discovered during code reviews suggests that secure coding practices are effectively integrated into the software development process. This means that systems are more resilient to attacks and less prone to errors.
- Faster and more frequent deployments – Increasing the frequency of deployments indicates the ability to deliver secure software faster. This is critical in dynamic IT environments where responding quickly to changing business requirements is essential.
- Increased compliance with security policies – Increased compliance with security policies means that businesses are better adhering to established security standards, which reduces the risk of data breaches and security incidents.
- Reduced false positives – Reducing false positives means that security monitoring systems are more accurate, allowing teams to focus on real-world threats and minimize unnecessary interventions.
- Increased security awareness – an increase in the percentage of employees who have completed security training indicates a higher level of security awareness in organizations. This helps to create a safety culture where every employee is aware of the risks and knows how to respond to them.
- Better user access management - Increasing the frequency of user access reviews helps ensure that only authorized users have access to critical resources, reducing the risk of unauthorized access.

Analyze the results

Interpreting the results in the context of the study objectives

The aim of the study was to understand the impact of DevSecOps on business continuity and resilience of IT systems. The results show that the implementation of DevSecOps has significantly improved these aspects, which confirms the hypotheses put forward at the beginning of the study. For example, the average response time to security incidents was reduced by 40% and the number of critical errors was reduced by 30%. These results are in line with previous studies that have also indicated the positive impact of DevSecOps on the security and continuity of systems. For example, research by Balas (2024) has shown similar benefits in the context of large tech companies. Our study expands on these results by showing that these benefits are also evident in medium and small businesses.

Analysis of potential limitations of the study and their impact on results

One of the main limitations of the study was the limited sample size, which may have affected the generalization of the results. Companies from the technology and academic sectors participated in the survey, which may mean that the results are not fully representative of other industries. In addition, the study was based on participants' self-assessment, which may introduce some reporting errors.

Proposals for further directions of research and development in the field

Moving forward, it is a clever idea to conduct research on a larger sample that spans different industries to better understand the impact of DevSecOps on different types of organizations. In addition, it would be interesting to explore how modern technologies such as artificial intelligence and machine learning can be integrated into DevSecOps to further enhance the security and continuity of systems.

Discussion

Discussion on the importance of the results and their practical implications

The results of the study indicate that the implementation of DevSecOps significantly improves the continuity and resilience of IT systems. Reducing the average response time to security incidents by 40% and reducing critical errors by 30% suggests that DevSecOps can be a key component of your IT business continuity and resilience security. The practical implications of these results include:

- Increase operational efficiency: Organizations can respond to threats faster by minimizing downtime and data loss.
- Improve software quality: Integrating security at every stage of the software lifecycle leads to the creation of more reliable and secure applications.
- Cost reduction: Early detection and correction of errors can reduce the costs associated with subsequent repairs and incident management.

Analysis of potential limitations of the study and their impact on results

Each test has its limitations, which can affect the interpretation of the results. For tours, the main restrictions include:

- The sample size - the study included five organizations, is insufficient to generalize the results for all sectors. A sample of lagers can provide more representative data.
- Participant self-assessment – the results were based on the participants' self-assessment, which may introduce some reporting errors. Future research may include more objective methods of data collection.
- Industry specifics – the study focused on technology and academic companies, which may mean that the results are not fully representative of other industries. It is a clever idea to conduct research across sectors to better understand the impact of DevSecOps.

Proposals for further directions of research and development in the field

The results of our study open several interesting directions for future research:

- Sample extension – Conduct research on a larger sample, spanning different industries, to better understand the impact of DevSecOps on different types of organizations.
- Modern Technology Integration – Exploring how modern technologies such as artificial intelligence and machine learning can be integrated with DevSecOps to further enhance the security and continuity of systems.
- Long-term impacts - Analyze the long-term impacts of implementing DevSecOps to understand how these practices affect organizations over several years.

Case studies of companies that have implemented DevSecOps

The following case studies show how various companies have successfully implemented DevSecOps to improve the security, reliability, and performance of their systems.

1. Company A, a leading technology company, has successfully implemented DevSecOps and has seen significant increases in deployment rates, reduced security incidents, and cost savings. It has increased the frequency of deployments from 4 per month to over 10, thanks to the use of Kubernetes.
2. Company D - A midsize manufacturing company implemented a DevSecOps approach using Azure DevOps, static code analysis, and vulnerability scanning. This reduced downtime to less than 3% and reduced errors by 85%.
3. C – Technical Academy integrated automated security tests in the development team, which allowed for faster detection and fixing of vulnerabilities. This allowed for faster response to threats and minimizing the risk of security incidents.

4. E – A university focused on training and building a safety culture in the team. Regular security training and promoting threat awareness among employees have helped to increase the resilience of systems and reduce the number of incidents.

These case studies show that implementing DevSecOps can bring significant benefits in terms of business continuity, cyber resilience, and operational efficiency. Findings from the global study by Oleg (2025) support these observations, indicating that organizations adopting DevSecOps report higher deployment frequency, reduced incident rates, and improved compliance outcomes across sectors.

Summary

DevSecOps plays a critical role in ensuring business continuity and resiliency of systems by integrating security at every stage of the GIS software lifecycle. With a DevSecOps approach, organizations can detect vulnerabilities and fix vulnerabilities faster, minimizing risk and increasing trust in GIS systems. Implementing DevSecOps requires a change in organizational culture, process automation, and continuous monitoring and testing of business continuity and resiliency of systems. Effective use of DevSecOps leads to more secure and reliable applications, which is essential in today's dynamic cyber environment – cyberspace. Research shows that organizations that have implemented DevSecOps have seen significant benefits. DevSecOps is not just a trend, but a necessity in today's cyber world.

From the conducted research and the description of several case studies for five companies, several key conclusions can be drawn:

- Companies that have implemented DevSecOps have seen a significant increase in the frequency of deployments. For example, one company increased the frequency of deployments from 4 per month to more than 10 using Kubernetes. Automation and CI/CD have contributed to faster and more efficient software delivery.
- The integration of security practices throughout the software lifecycle (SDLC) has helped reduce the number of security incidents. Companies reported fewer vulnerabilities and responded faster to threats.1
- The implementation of DevSecOps has contributed to improving code quality through regular code reviews and automated security testing. Companies have seen a reduction in bugs and security issues.
- DevSecOps promotes collaboration between development, operations, and security teams. Better communication and coordination have contributed to more effective project management and faster problem resolution.
- Companies have seen savings through process automation, reduced security incidents, and faster software delivery. In one case, the company reduced downtime to less than 2% and reduced errors by 85%.
- DevSecOps has helped companies achieve compliance with regulations and security standards faster. Automation of compliance processes and regular audits have contributed to better risk management.

These results also show that implementing DevSecOps can bring significant benefits in terms of security, quality, performance, and cost.

Unlike traditional DevOps, which primarily focuses on rapid software delivery and collaboration between development and operations teams, DevSecOps adds a security aspect to the equation. By working closely with development, operations, and security teams to automate processes, DevSecOps enables faster, more reliable, and secure GIS deployments. As a result, DevSecOps not only increases operational efficiency but also contributes to the long-term success of the organization.

Implementing DevSecOps comes with some challenges. Changing organizational culture is one of the main challenges, as it requires breaking down silos and introducing a culture of collaboration. This requires the involvement of all team members and the support of management. Based on the results and discussions, new research questions

emerged, such as: (1) What are the long-term effects of implementing AI in DevSecOps? (2) What are the best practices for implementing AI in different industry contexts? (3) What are the specific challenges of integrating AI in DevSecOps in SMBs?

References

- Abdiukov, T. (2024) 'Automated security testing in DevSecOps pipelines: Integrating AI-based vulnerability discovery and compliance validation', *World Journal of Advanced Research and Reviews*, 22(1), pp. 2083–2093. DOI: https://doi.org/10.30574/wjarr.2024.22.1.1083
- ATARC DevSecOps Working Group (2025) *DevSecOps Maturity Model for Federal Government Agencies*. Advanced Technology Academic Research Center. Available at: https://atarc.org/wp-content/uploads/2025/05/atarc-wp-devsecops-maturity-model-for-federal-government-agencies_5.15-1.pdf
- Balas, A. (2024) 'DevSecOps Implementation in Medium-Sized Enterprises: A Comparative Study', *International Journal of Information Security*, 23(4), pp. 3765–3788. DOI: https://doi.org/10.1007/s10207-024-00909-w
- Binbeshr, F. and Imam, M. (2025) *Comparative Analysis of AI-Driven Security Approaches in DevSecOps: Challenges, Solutions, and Future Directions*. *arXiv preprint*, arXiv:2504.19154. Available at: https://arxiv.org/html/2504.19154v1
- Cybersecurity Ventures (2024) *Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics*. Available at: https://cybersecurityventures.com/cybersecurity-almanac-2024/
- Department of Defense (DoD) (2021) *DoD Enterprise DevSecOps Strategy Guide*. Version 2.0. Available at: https://dl.dod.cyber.mil/wp-content/uploads/devsecops/pdf/DoDEnterpriseDevSecOpsStrategyGuide.pdf
- Fu, M., Pasuksmit, J. and Tantithamthavorn, C. (2024) *AI for DevSecOps: A Landscape and Future Opportunities*. Monash University & Atlassian. Available at: https://arxiv.org/pdf/2404.04839
- Gbenle, P., Olayemi, A., and Adepoju, A. (2025) 'A DevSecOps-Centered Conceptual Model for Continuous Integration and Secure Deployment in Software Development Lifecycles', *World Scientific News*, 203, pp. 336–373. Available at: https://worldscientificnews.com/wp-content/uploads/2025/05/WSN-203-2025-336-373.pdf
- GitLab (2024) *The GitLab 2024 Global DevSecOps Report*. ReleaseTEAM. Available at: https://www.releaseteam.com/wp-content/uploads/2024-GitLab-Global-DevSecOps-Report-ReleaseTEAM.pdf
- GovCIO Media & Research (2025) 'Feds Turn to DevSecOps to Balance Innovation with Public Trust', *GovCIO*, 6 August. Available at: https://govciomedia.com/feds-turn-to-devsecops-to-balance-innovation-with-public-trust/
- IBIMA (2025) *The Role of DevSecOps in Ensuring Business Continuity and Resiliency of GIS Systems*. 46th IBIMA Computer Science Conference, Ronda, Spain. Available at: https://ibima.org/accepted-paper/the-role-of-devsecops-in-ensuring-business-continuity-and-resiliency-of-gis-systems/
- Oleg, S. (2025) *DevSecOps Implementation Impact: Global Study 2025*. *GetTrusted Blog*. Available at: https://gettrusted.io/blog/devsecops-implementation-impact-global-study-2025/
- Prates, D. and Pereira, R. (2024) 'A multivocal literature review on DevSecOps practices and tools', *Journal of Systems and Software*, 200, pp. 1–15. DOI: https://doi.org/10.1016/j.jss.2024.111678
- Rodriguez, J., Silva, M. and Costa, L. (2024) 'A DevSecOps maturity model for secure software delivery', *Software Quality Journal*, 32(3), pp. 455–478. DOI: https://link.springer.com/article/10.1007/s11219-024-09654-3
- Sandu, A.K. (2021) 'DevSecOps: Integrating Security into the DevOps Lifecycle for Enhanced Resilience', *Technology & Management Review*, 6(1). Available at: https://upright.pub/index.php/tmr/article/view/131
- Smith, J. and Brown, L. (2022) 'DevSecOps: Integrating Security Across the Software Lifecycle', *International Journal of Computer Trends and Technology*, 70(6), pp. 19–23. DOI: https://doi.org/10.14445/22312803/IJCTT-V70I6P102
- Synopsys Cybersecurity Research Center (2023) *Global State of DevSecOps 2023*. Synopsys, Inc. Available at: https://investor.synopsys.com/news/news-details/2023/New-Synopsys-Research-Reveals-Vast-Majority-of-Organizations-Report-DevOps-Delays-Due-to-Critical-Security-Issues/default.aspx
- Veeramachaneni, V. (2023) 'A Systematic Review of DevSecOps: Bridging Security and Agile Development for Resilient Software Systems', *NeuroQuantology*, 21(7), pp. 1251–1255. DOI: https://doi.org/10.48047/nq.2023.21.7.nq23114