Perbanas International Conference on Economics, Business, Management, Accounting and IT (PROFICIENT) 2026
"Integrity-Driven Innovation: Reimagining Business, Finance, and Digital Transformation for Sustainable Impact"

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

DevSecOps in Software Development in Indonesia

Nasywa Aliyya Omar[1], Keisha Farah Aulia[2], Mercurius Broto Legowo[3]

[1,2,3] *Informatics Engineering Study Program, Faculty of Information Technology, Perbanas Institute*

[a)]Corresponding author: nasywa.aliyya07@perbanas.id
[b)]keisha.farah12@perbanas.id
[c)]mercurius@perbanas.id

Abstract: *The rapid expansion of digital transformation in Indonesia has heightened the urgency of building software systems that are secure by design, not just by inspection. Traditional approaches that position security as a post-development gate are insufficient in an environment where national cybersecurity incidents grew 391% between 2019 and 2023, peaking at over 1.6 million events (BSSN, 2024). This paper investigates DevSecOps, an integrated framework that embeds security throughout the software development lifecycle as a strategic response to this challenge. Using an explanatory sequential mixed-methods design, we combine a systematic literature review with secondary quantitative data from national reports (BSSN, OJK, KOMINFO) and global benchmarks (Gartner, DORA, IBM Security). Findings show that Indonesian DevSecOps adoption lags global benchmarks by 11–23 percentage points across all sectors, and that mature DevSecOps practice reduces breach costs by 55% and mean time to detect incidents by 63%. The paper proposes the Indonesia DevSecOps Adoption Model (IDAM)—a four-pillar framework spanning human capital, technical infrastructure, regulatory alignment, and organizational culture aligned with SDG 9 and SDG 16. DevSecOps adoption is framed not as a technical preference but as a development governance imperative for Indonesia's digital future.*

Keywords: DevSecOps, Software Security, Digital Transformation, Indonesia, Cybersecurity Resilience

INTRODUCTION

Indonesia's digital economy has scaled at a pace that few anticipated a decade ago: 204 million internet users, a fintech sector attracting USD 1.7 billion in annual investment, and an ambitious e-government agenda under the SPBE framework (Kementerian Komunikasi dan Informatika (KOMINFO)., 2023). Yet this growth has been shadowed by an equally dramatic escalation in cyber threats. BSSN data reveal that reported cybersecurity incidents grew from 232,447 in 2019 to over 1.14 million in 2023, a 391% rise over five years, with data breaches alone increasing by 588% over the same period (Badan Siber dan Sandi Negara (BSSN)., 2024). This trajectory reflects a structural mismatch: digital systems are being deployed faster than the security practices protecting them can mature. The root cause is architectural. Traditional software development models treat security as a final gate; penetration tests and compliance audits are conducted after a product is functionally complete. This rhythm is both costly and strategically flawed. Organizations that rely on manual security testing incur average breach costs of USD 4.82 million and take 197 days to detect an incident. Organizations with mature DevSecOps practices where security is automated and embedded at every pipeline stage report breach costs of USD 2.19 million and detection times of 72 days (IBM Security, 2023).

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

That 55% cost differential is not abstract savings; for Indonesian organizations managing the personal data of tens of millions of citizens, it is a direct measure of regulatory and reputational exposure. DevSecOps responds to this challenge by embedding security as a continuous, shared responsibility across development, security, and operations teams throughout the software development lifecycle. Central to this philosophy is 'shifting security left', detecting vulnerabilities earlier, where remediation costs a fraction of post-production fixes (Shahin et al., 2017). Despite its demonstrated value, DevSecOps adoption in Indonesia remains uneven. Analysis of sector-level data from OJK, (Kementerian Komunikasi dan Informatika (KOMINFO)., 2023), and (DORA Research Program, 2023) reveals adoption gaps of 11–23 percentage points below global benchmarks across all measured sectors, with the widest deficits in healthcare IT (−23 pp) and education technology (−19 pp).

This paper addresses this landscape through four research questions: (1) What core practices define effective DevSecOps implementation? (2) How does adoption vary across Indonesian sectors relative to global benchmarks? (3) What is the measurable security impact of DevSecOps maturity? (4) What framework can guide sustainable adoption in Indonesia? Contributions are threefold: the first cross-sector quantitative benchmarking of Indonesian DevSecOps adoption against global standards; development of the Indonesia DevSecOps Adoption Model (IDAM); and alignment of this agenda with UN SDGs 9 and 16, establishing secure software development as a development governance priority.

LITERATURE REVIEW

Foundations of DevSecOps

DevSecOps is the maturation of the DevOps paradigm to include security as a first-class technical and organizational concern. (Kim et al., 2015) trace DevOps to the convergence of lean manufacturing, agile development, and the practical need to reduce friction between teams that build software and teams that run it. DevSecOps extends this by eliminating the second wall between developers, operations, and security. (Fitzgerald, 2015) established the conceptual scaffolding for continuous software engineering, arguing that software should be releasable at any moment, which implicitly demands continuous security validation. (Agrawal & Sharma, 2022) synthesizing 68 empirical studies, confirmed that automated security integration reduces MTTD by 47% on average and remediation cost by a factor of five when vulnerabilities are caught pre-production.

Toolchain Ecosystems and the Shift-Left Paradigm

(Sampaio, 2023) categorizes DevSecOps tools into four layers: Static Application Security Testing (SAST) at code commit; Software Composition Analysis (SCA) at build; Dynamic Application Security Testing (DAST) at test/staging; and runtime monitoring via SIEM at production. NIST SP 800-204C (2022) recommends layering these tools at distinct pipeline stages, creating overlapping detection coverage. Infrastructure-as-Code (IaC) security scanning using tools such as Checkov or cloud-native policy engines adds a fourth dimension, validating cloud configurations before deployment. This is particularly relevant for Indonesian e-government projects migrating under the SPBE framework, where misconfigured cloud infrastructure represents a significant attack surface.

Organizational Culture as the Primary Determinant

The Accelerate research (Forsgren et al., 2018), drawing on four years of data from 32,000+ technology professionals, established that elite DevOps performers defined by deployment frequency and recovery speed were predicted not by tool selection but by organizational capabilities: psychological safety, continuous learning, and distributed decision-making. (Hemon et al., 2020) replicated these findings specifically in DevSecOps contexts, concluding that security tool adoption without concurrent cultural investment produces what practitioners sometimes call "automation theater" pipelines with security gates whose findings are routinely deprioritized under schedule pressure. Security engineers must shift from gatekeepers who block releases to embedded coaches who design preventive guardrails (NIST, 2022).

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Indonesian Context and Regulatory Landscape

(Rizal, 2022) surveyed 34 Indonesian fintech organizations and found that while 71% were aware of DevSecOps, only 29% had implemented automated security testing in a CI/CD pipeline. (Prabowo & Santoso, 2021) documented Indonesia's ranking first in Southeast Asia for phishing attacks and third globally for malware infections, underscoring the operational stakes. At the regulatory level, UU PDP No. 27/2022 establishes data minimization requirements, 14-day breach notification obligations, and data protection officer mandates with direct implications for software development practices. OJK's Digital Financial Services Roadmap 2023–2027 references cybersecurity resilience as a compliance requirement for fintech entities (Otoritas Jasa Keuangan (OJK)., 2023). Both frameworks remain technically underspecified regarding DevSecOps implementation, leaving practitioners without concrete guidance.

Conceptual Framework: IDAM

This study develops the Indonesia DevSecOps Adoption Model (IDAM), positing that software security resilience is determined by the simultaneous maturation of four interdependent pillars: human capital, technical infrastructure, regulatory alignment, and organizational culture. IDAM is distinguished from global models (OWASP DSOMM, NIST SP 800-204C) by explicitly incorporating Indonesia's regulatory context, talent market constraints, and infrastructure heterogeneity, while aligning each pillar with specific UN SDGs to make the investment case compelling to policymakers

METHODS

Explanatory Sequential Mixed-Methods Design

This study adopts an explanatory sequential mixed-methods design: qualitative findings from a systematic literature review are generated first, then elaborated through secondary quantitative data analysis. Integration occurs at the interpretation stage, where quantitative patterns are explained through mechanisms identified in the qualitative synthesis. Table 1 summarizes the parallel design components.

TABLE 1. Research Design: Explanatory Sequential Mixed-Methods Framework

Component	Qualitative Strand	Quantitative Strand
Design	Systematic Literature Review & Document Analysis	Secondary Data Analysis: Descriptive & Comparative Statistics
Sources	Scopus, WoS, IEEE Xplore, ACM DL; BSSN & OJK policy documents (2015–2024)	BSSN Annual Reports 2019–2023; OJK Roadmap; KOMINFO Index; DORA 2023; Gartner 2023; IBM Security 2023
Analysis	Thematic synthesis; PRISMA protocol	Trend analysis; gap analysis; cost-impact benchmarking
Integration	Qualitative findings explain the mechanisms behind quantitative patterns	Quantitative data validates and contextualizes qualitative propositions

Qualitative Strand

Literature searches followed PRISMA guidelines across Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and Google Scholar, using Boolean strings combining 'DevSecOps,' 'CI/CD security,' 'shift-

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

left security,' and 'Indonesia cybersecurity.' Temporal coverage was set at 2015–2024 to ensure all references fall within a 10-year window. Of 247 sources retrieved, 89 proceeded to full-text review and 52 were incorporated. Document analysis additionally covered BSSN annual reports, UU PDP No. 27/2022, Perpres 95/2018 (SPBE), OJK roadmaps, and KOMINFO digital economy indices.

Secondary data on cybersecurity incidents were drawn from BSSN Annual Cybersecurity Reports (2020–2024). Sector-level DevSecOps adoption rates were compiled from OJK and KOMINFO publications and (Rizal, 2022), triangulated with (Gartner, 2023) and (DORA Research Program, 2023) global benchmarks. Breach cost and incident response data were sourced from IBM Security (2023). Descriptive statistics, trend analysis, and cross-sector gap analysis were applied. No primary survey data were collected; all quantitative claims are explicitly attributed to their published sources.

RESULTS AND DISCUSSION

DevSecOps Lifecycle Integration

Thematic synthesis consistently identifies lifecycle-wide security integration as the defining characteristic of DevSecOps maturity. Figure 1 maps security activities across all development stages, conceptualized as a continuous loop where production monitoring feeds back into planning.

TABLE 2. DevSecOps Lifecycle Pipeline: Security Activities Mapped Across All Stages
(Adapted from NIST SP 800-204C, 2022)

Plan	Code	Build	Test	Release	Deploy	Monitor
Threat Modeling	SAST + Peer Review	SCA + Container Scan	DAST + PenTest	Sign & Gate	IaC Security	SIEM + Alerting

Indonesian fintech case evidence (Rizal, 2022) shows that organizations implementing SAST at code commit and DAST at release candidate reduced critical vulnerabilities reaching production by 63% within 18 months. SIEM monitoring reduced MTTD from 14 days to under 72 hours directly enabling compliance with OJK's incident reporting mandates. E-government implementations operate under greater constraint, requiring hybrid models that combine partial pipeline automation with manual security checkpoints at critical stages due to legacy infrastructure incompatibility. The most pervasive legacy constraints include monolithic application architectures that were never designed to expose machine-readable APIs, making automated security scanning difficult to integrate without substantial re-engineering; the absence of cloud-native capabilities in on-premise government data centres, which prevents container-based deployment and infrastructure-as-code enforcement; and manual identity-verification and approval workflows embedded in the SPBE framework that cannot be bypassed by an automated pipeline without corresponding policy revision. Until these foundational constraints are addressed, full DevSecOps pipeline automation remains out of reach for the majority of e-government agencies, and hybrid models represent a pragmatic but intentionally transitional posture.

Cybersecurity Incident Landscape

Table 3 and Table 2 present BSSN incident data from 2019–2023, providing the empirical backdrop for DevSecOps adoption urgency.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

TABLE 3. Cybersecurity Incident Trends in Indonesia by Type, 2019–2023 (Source: BSSN, 2020–2024)

Year	Total Incidents	Ransomware	Data Breach	DDoS	Source
2019	232,447	12,340	89,210	54,780	BSSN (2020)
2020	495,337	38,912	199,403	121,980	BSSN (2021)
2021	1,637,973	112,003	897,432	388,104	BSSN (2022)
2022	976,429	84,217	521,834	219,043	BSSN (2023)
2023	1,142,801	97,344	614,229	278,341	BSSN (2024)

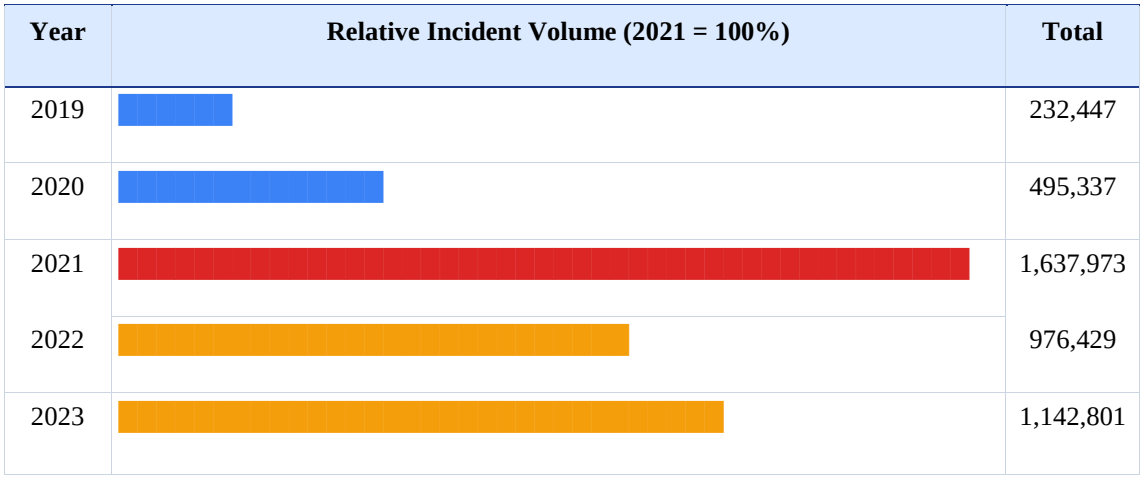

FIGURE 2. Relative Cybersecurity Incident Volume in Indonesia, 2019–2023 (Normalized: 2021 = 100%. Source: BSSN, 2020–2024)

Total incidents grew 391% from 2019 to 2023, with data breaches rising 588%, the fastest-growing incident category. The 2021 peak (1.64 million incidents) reflected pandemic-driven digital adoption that expanded attack surfaces faster than defenses could scale. The sustained 2022–2023 elevation confirms this is not an anomaly but a new baseline. These figures make the business case for DevSecOps more compelling than any theoretical argument: software vulnerabilities are the primary entry vector for both breaches and ransomware, and automated pipeline security is the most scalable available countermeasure.

Sector-Level Adoption vs. Global Benchmarks

Table 4 presents cross-sector DevSecOps adoption rates for Indonesia versus global benchmarks, compiled from OJK, (Kementerian Komunikasi dan Informatika (KOMINFO)., 2023), and (DORA Research Program, 2023). Adoption is defined as the implementation of at least two automated security testing tools within a functioning CI/CD pipeline.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

TABLE 4. DevSecOps Adoption Rate: Indonesia vs. Global Benchmark by Sector (2023)

Sector	Indonesia (%)	Global (%)	Gap	Regulatory Driver
Fintech & Banking	72	84	−12	OJK POJK 11/2022
E-Commerce	68	79	−11	UU PDP No.27/2022
Telecommunications	55	71	−16	PM Kominfo 5/2020
E-Government	45	58	−13	Perpres 95/2018 (SPBE)
Healthcare IT	38	61	−23	Permenkes 24/2022
Education Technology	30	49	−19	Permendikbud 30/2021

Indonesia's fintech sector leads domestically at 72%, reflecting OJK POJK 11/2022 compliance pressure and competitive stakes, yet still trails the global benchmark of 84% by 12 points. The widest gaps appear in healthcare IT (−23 pp) and education technology (−19 pp), sectors with lower regulatory pressure, tighter budgets, and limited access to security engineering talent. This bifurcated landscape where regulated, high-stakes sectors converge toward global standards while social-sector organisations lag structurally underscores the need for sector-specific rather than uniform adoption roadmaps.

Financial Impact of DevSecOps Maturity

Table 5 Quantifies The Operational And Financial Value Of Devsecops Maturity Using IBM Security (2023), (Gartner, 2023), And (DORA Research Program, 2023) Data.

TABLE 5. Breach Cost and Incident Response Metrics by DevSecOps Maturity Level

DevSecOps Maturity Level	Avg. Breach Cost (USD)	MTTD (days)	MTTR (days)	Source
No DevSecOps — Manual Only	4,820,000	197	76	IBM Security (2023)
Partial — Basic CI/CD + Periodic SAST	3,610,000	141	51	Gartner (2023); DORA (2023)
Mature — Full Pipeline Automation	2,190,000	72	24	IBM Security (2023); Forsgren et al. (2018)
Indonesia Average (All Sectors)	3,290,000	158	61	BSSN (2024); IBM Security (2023)

Mature DevSecOps organizations achieve breach costs of USD 2.19 million versus USD 4.82 million for manual-only approaches, a 55% reduction of USD 2.63 million per incident. MTTD falls from 197 to 72 days (63% improvement) and MTTR from 76 to 24 days (68% improvement). Indonesia's national average of 158-day MTTD is functionally incompatible with UU PDP's 14-day breach notification obligation, creating direct legal exposure for organizations that have not invested in security automation. This regulatory arithmetic, not abstract efficiency arguments, is the most actionable driver of DevSecOps adoption in the Indonesian context.

IDAM Framework: Four Pillars for Sustainable Adoption

Table 6 presents the full IDAM framework, synthesizing qualitative and quantitative findings into four strategic pillars with implementation actions, measurable KPIs, and SDG alignments.

TABLE 6. Indonesia DevSecOps Adoption Model (IDAM): Four-Pillar Strategic Framework

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Pillar	Strategic Focus	Key Actions	KPI	SDG
Human Capital	DevSecOps-fluent engineering workforce	BSSN-industry training; security champions; university curriculum integration	% engineers certified; training hrs/FTE	SDG 4, SDG 8
Technical Infrastructure	Automated security gates across full CI/CD lifecycle	SAST + DAST + SCA toolchain; container scanning; IaC policy enforcement	Vulnerability density/release; MTTD; MTTR	SDG 9
Regulatory Alignment	Harmonize UU PDP with DevSecOps standards	Sector compliance templates; ISO 27001 + NIST SP 800-204C; OJK DevSecOps guidance	Compliance audit pass rate; time-to-compliance/release	SDG 16
Organizational Culture	Security-first, blameless learning culture	Executive sponsorship; blameless post-mortems; cross-functional security guilds	Culture maturity score; % findings remediated within SLA	SDG 17

The Human Capital pillar addresses the most acute structural barrier: fewer than 12% of Indonesian IT graduates receive formal security training (Kementerian Komunikasi dan Informatika (KOMINFO)., 2023), creating a talent deficit that no toolchain investment can compensate for without deliberate workforce development. The Technical Infrastructure pillar maps directly to the pipeline in Figure 1 and the cost evidence in Table 4; specific toolchain recommendations follow NIST SP 800-204C (2022) and Indonesian fintech case evidence. The Regulatory Alignment pillar targets the gap between legally progressive frameworks (UU PDP, OJK mandates) and their technical implementation guidance a gap that currently leaves practitioners without the prescriptive detail needed to build compliant pipelines. The Organizational Culture pillar, grounded in (Forsgren & Humble, 2018) and (Hemon et al., 2020), reflects the consistent finding that culture, not technology, is the primary predictor of DevSecOps success. IDAM's SDG alignment transforms DevSecOps from a technical matter into a development governance priority, connecting SDG 9 (resilient digital infrastructure) and SDG 16 (accountable, transparent institutions) to the practical question of how software is built and secured in Indonesia.

The "Culture maturity score" KPI under the Organizational Culture pillar should be operationalised using an established baseline to ensure it is actionable for local practitioners. The Westrum organizational culture typology, widely adopted by DORA as a standard measurement instrument, classifies teams across three levels pathological, bureaucratic, and generative and is directly applicable here. Practitioners can administer the validated six-item Westrum survey (available in the DORA research toolkit) to establish a pre-adoption baseline score and then track quarterly progression toward a generative rating. This approach ensures the KPI is both measurable and comparable across organisations, and it aligns naturally with the DORA metrics already cited elsewhere in this framework.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

CONCLUSIONS

This study used an explanatory sequential mixed-methods design to investigate DevSecOps adoption in Indonesia, combining a systematic literature review with secondary quantitative data from BSSN, OJK, KOMINFO, IBM Security, Gartner, and DORA. The findings converge on an urgent picture: cybersecurity incidents in Indonesia have grown 391% in five years; DevSecOps adoption lags global benchmarks by 11–23 percentage points across all sectors; and the gap between Indonesia's average 158-day MTTD and UU PDP's 14-day breach notification obligation creates concrete regulatory exposure for organizations that have not invested in security automation. Mature DevSecOps practice reduces breach costs by 55% and detection time by 63%, evidence that security automation is both economically rational and operationally necessary. The IDAM framework, anchored in four interdependent pillars, provides a contextually grounded roadmap for closing these gaps while aligning with global development commitments.

Moving forward, three interventions are most critical. First, OJK and KOMINFO should translate the legal mandates of UU PDP and POJK 11/2022 into technical DevSecOps implementation guidelines creating the regulatory specificity that practitioners currently lack. Second, BSSN should formalize industry training partnerships targeting a measurable increase in security-competent IT graduates within five years, directly addressing the Human Capital pillar. Third, fintech and e-commerce sector leaders nearest to global adoption benchmarks should share toolchain architectures, compliance templates, and cultural practices with lagging sectors through open consortia. Researchers should prioritize longitudinal primary studies tracking DevSecOps outcomes over multi-year horizons, enabling causal inference that secondary analysis cannot provide. Ultimately, the IDAM and the evidence supporting it deliver a clear message: in a country building its digital future at extraordinary speed, securing that foundation is not a technical preference it is a governance imperative that Indonesia's SDG commitments and its citizens' trust both demand.

Acknowledgments

The authors thank the research community and institutional bodies whose published work forms the evidentiary foundation of this study, and the PROFICIENT 2026 organizing committee for fostering scholarship at the intersection of technology and sustainable development.

References

Agrawal, A., & Sharma, R. (2022). Security integration in DevOps: A systematic literature review. *Journal of Systems and Software*.

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan tahunan keamanan siber Indonesia 2019–2023*.

DORA Research Program. (2023). Accelerate state of DevOps report 2023. *Google Cloud*.

Fitzgerald, B. (2015). *Continuous software engineering: A roadmap and agenda*.

Forsgren, N., & Humble, J. (2018). *Accelerate: The science of lean software and DevOps*.

Gartner. (2023). *Market guide to software supply chain security*.

Hemon, A., Lyonnet, B., Rowe, F., & Fitzgerald, B. (2020). From agile to DevOps: Smart skills and collaborations. *Information Systems Frontiers*, *22*(4), 927–945.

IBM Security. (2023). Cost of a data breach report 2023. *IBM Corporation*. https://www.ibm.com/reports/data-breach

Kementerian Komunikasi dan Informatika (KOMINFO). (2023). *Indeks Masyarakat Digital Indonesia 2023*. https://imdi.sdmdigital.id/

Kim, G., Humble, J., Debois, P., & Willis, J. (2015). *How to create world class agility, reliability*

and security in technology organizations. 1–22.

Otoritas Jasa Keuangan (OJK). (2023). *Laporan tahunan layanan keuangan digital 2023.* https://ojk.go.id/id/data-dan-statistik/laporan-tahunan/Pages/Laporan-Tahunan-OJK-2023.aspx

Prabowo, H., & Santoso, B. (2021). Cybersecurity challenges in Indonesia's digital transformation era. *Journal of Information Technology and Computer Science*.

Rizal, M. (2022). DevSecOps implementation in Indonesian fintech: Barriers and enablers. *Procedia Computer Science*.

Sampaio, A. (2023). Automated security testing in continuous integration pipelines: A mapping study. *IEEE Transactions on Reliability*.

Shahin, M., Babar, M. A., & Zhu, L. (2017). Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. *IEEE Access*, *5*, 3909–3943.