BAB I
PENDAHULUAN

A. Latar Belakang Penelitian

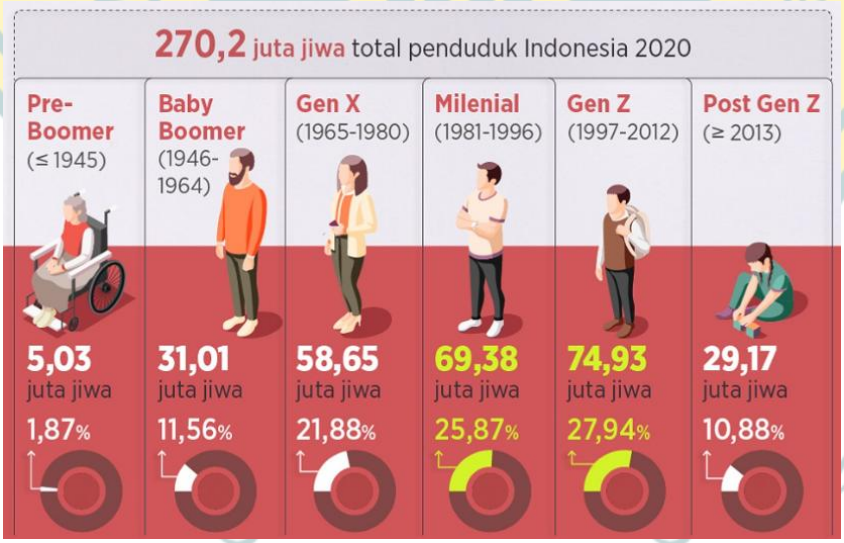
Perkembangan transformasi digital telah mendorong terjadinya perubahan yang sangat signifikan dalam cara organisasi beroperasi, berkolaborasi, dan berkomunikasi. Bisnis yang mampu bertahan dan tumbuh dalam konteks ini semakin bergantung pada teknologi informasi dan komunikasi (TIK) sebagai enabler utama untuk mempercepat inovasi produk, meningkatkan efisiensi operasional, serta merespons dinamika pasar secara lebih cepat dan adaptif. Dalam perspektif manajemen strategis, TIK tidak lagi dipandang semata-mata sebagai infrastruktur pendukung, melainkan sebagai bagian integral dari strategi organisasi yang mengharuskan integrasi erat antara teknologi dan proses bisnis inti. Dengan demikian, adopsi teknologi diproyeksikan tetap menjadi salah satu pendorong utama transformasi bisnis dalam beberapa tahun ke depan.

Perkembangan perangkat lunak secara lebih spesifik menunjukkan evolusi yang sangat pesat dalam beberapa dekade terakhir. Berawal dari program sederhana yang berjalan pada lingkungan mainframe, perangkat lunak berkembang menjadi ekosistem yang kompleks, terdistribusi, dan saling terhubung dalam jaringan. Inovasi seperti sistem operasi modern, aplikasi berbasis layanan, dan komputasi awan (*cloud computing*) telah mengubah cara individu dan organisasi bekerja, berkomunikasi, serta mengakses dan memanfaatkan informasi secara fundamental. Dalam praktik kontemporer, produk perangkat lunak banyak dikembangkan secara iteratif dan inkremental menggunakan pendekatan *agile*, di-*deploy* pada lingkungan *cloud*, dilengkapi dengan mekanisme keamanan sistem yang lebih komprehensif, serta dikelola secara berkelanjutan oleh tim lintas fungsi seperti DevOps (Sommerville, 2020). Selain itu, kemajuan dalam bidang kecerdasan buatan dan *machine learning* memungkinkan munculnya perangkat lunak yang tidak hanya menjalankan instruksi secara statis, tetapi juga mampu belajar dari data dan beradaptasi secara mandiri terhadap konteks dan kebutuhan pengguna (Norvig & Russell, 2021). Kondisi ini menegaskan bahwa perangkat lunak telah menjadi

tulang punggung revolusi digital dan menjadi fondasi bagi berbagai perkembangan teknologi mutakhir, mulai dari kecerdasan buatan hingga *Internet of Things*.

Ekspektasi pengguna perangkat lunak juga mengalami peningkatan dan perubahan karakteristik. Generasi digital yang tumbuh dan berkembang dalam era dominasi komputer, internet, dan perangkat bergerak yang secara umum mencakup mereka yang lahir sejak dekade 1980-an hingga sekarang memiliki standar pengalaman penggunaan (*user experience*) yang lebih tinggi. Mereka menuntut antarmuka yang intuitif, kinerja yang responsif, serta layanan yang bersifat personal dan kontekstual. Kesadaran pengguna terhadap isu keamanan informasi dan privasi data semakin menguat.

Pengguna tidak hanya mengharapkan perangkat lunak yang fungsional dan mudah digunakan, tetapi juga menuntut jaminan keamanan dan perlindungan terhadap data pribadi agar tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang. Kombinasi tuntutan terhadap kecepatan, kualitas, dan keamanan ini mendorong organisasi untuk merancang, mengembangkan, dan mengimplementasikan perangkat lunak yang lebih baik, lebih cepat, dan lebih aman, sehingga mampu menjawab kebutuhan pemangku kepentingan di era transformasi digital yang kian kompleks.



Gambar 1. 1 Indonesia Didominasi Milenial dan Generasi Z
Bayu, D. J. (2021, January 30). Indonesia Didominasi Milenial dan Generasi Z - Infografik Katadata.co.id. (Bayu, 2021)

Banyak organisasi telah beralih pada pendekatan pengembangan perangkat lunak yang lebih gesit dan responsif untuk memenuhi ekspektasi kinerja, kecepatan, dan kualitas yang semakin tinggi. Salah satu pendekatan yang menonjol adalah DevOps, sebuah paradigma yang mengintegrasikan fungsi pengembangan (*Development*/Dev) dan operasi (*Operations*/Ops) guna membangun proses pengembangan sistem yang lebih efisien, kolaboratif, dan adaptif. Praktik DevOps menekankan otomatisasi, pengujian berkelanjutan (*continuous testing*), integrasi dan pengiriman berkelanjutan (*continuous integration*/*continuous delivery*), serta kolaborasi yang erat antara tim pengembang dan tim operasi sehingga mengurangi hambatan struktural maupun koordinatif di antara keduanya.

Dalam praktik tradisional, pemisahan yang tegas antara tim pengembangan (*developer*) dan tim operasi (*operations*) kerap menimbulkan berbagai persoalan. Tim pengembangan berfokus pada penciptaan dan penyempurnaan fitur perangkat lunak, sedangkan tim operasi bertanggung jawab mengelola infrastruktur dan menjaga stabilitas layanan. Perbedaan fokus dan indikator kinerja ini sering berujung pada ketidaksinkronan tujuan, konflik kepentingan, keterlambatan peluncuran produk, serta meningkatnya kerentanan, termasuk di aspek keamanan sistem. Dengan kata lain, model kerja yang terfragmentasi berpotensi menghambat pencapaian tujuan organisasi dalam menghadirkan layanan digital yang andal dan aman.

Perubahan menuju pendekatan pengembangan yang lebih cepat dan iteratif juga membawa konsekuensi berupa tantangan baru di bidang keamanan perangkat lunak. Dalam banyak kasus, keamanan belum terintegrasi secara memadai ke dalam siklus hidup pengembangan perangkat lunak, sehingga isu keamanan baru teridentifikasi di tahap akhir, atau bahkan setelah sistem dioperasikan. Kondisi ini tidak hanya meningkatkan biaya perbaikan, tetapi juga dapat menimbulkan kerugian signifikan bagi organisasi, baik dari sisi finansial, reputasi, maupun kepatuhan regulasi. Untuk merespons tantangan tersebut, lahirlah konsep DevSecOps yang mengintegrasikan dimensi keamanan (*Security*/Sec) ke dalam setiap tahap pengembangan dan operasional perangkat lunak.

DevSecOps memposisikan keamanan sebagai bagian integral dari proses dan budaya pengembangan, bukan sekadar tanggung jawab unit atau tim keamanan yang berdiri sendiri. Seluruh pemangku kepentingan yaitu *developer*, *operations*, serta *security* didorong untuk berbagi tanggung jawab dalam memastikan bahwa aspek keamanan terinternalisasi sejak tahap perancangan, pengembangan, pengujian, hingga *deployment* dan operasional. Implementasi DevSecOps yang efektif menuntut ketersediaan sumber daya manusia yang kompeten, baik dari sisi pengetahuan teknis maupun pemahaman terhadap praktik-praktik keamanan modern yang selaras dengan kebutuhan bisnis.

Sumber daya manusia (SDM) di bidang teknologi informasi dalam konteks ini dituntut untuk senantiasa mengikuti perkembangan teknologi dan beradaptasi secara cepat terhadap perubahan. Mereka perlu mengembangkan kompetensi yang relevan dengan tuntutan bisnis sekaligus memenuhi standar kinerja yang ditetapkan organisasi. Untuk mencapai target kinerja tersebut, upaya peningkatan kompetensi melalui *upskilling* dan *reskilling* bagi SDM TI menjadi kebutuhan strategis yang tidak dapat ditunda.

Ketersediaan talenta digital yang kompeten di Indonesia saat ini masih menghadapi kesenjangan yang cukup besar. Berdasarkan data Okupasi Nasional di Bidang Teknologi Informasi dan Komunikasi (TIK), kebutuhan SDM TI dilaporkan belum terpenuhi hampir di seluruh kategori jabatan. Kualitas pendidikan di bidang TIK di Indonesia juga masih relatif tertinggal, di mana Indonesia menempati peringkat ke-8 di kawasan Asia Tenggara, yang berimplikasi pada terbatasnya pasokan tenaga kerja kompeten di industri TIK (KOMINFO, 2017). Diproyeksikan bahwa Indonesia memerlukan sekitar 9 juta talenta digital pada tahun 2030, atau setara dengan kebutuhan sekitar 600 ribu talenta digital baru setiap tahunnya. Saat ini, perguruan tinggi di Indonesia hanya mampu menghasilkan sekitar 100.000–200.000 talenta digital per tahun, sehingga terdapat gap sekitar 400.000–500.000 talenta digital per tahun (Media, 2023).

Dalam konteks kebutuhan jabatan spesifik, *Software Engineer* tercatat sebagai salah satu dari tiga besar posisi TIK yang paling dibutuhkan, selain *Network Operation Access* dan *Network Operation Backbone* (KEMNAKER, 2021). Kondisi ini mengindikasikan urgensi pengembangan model pelatihan dan skema

pengembangan kompetensi yang lebih terstruktur dan kontekstual, termasuk di dalamnya penguatan kompetensi DevOps dan DevSecOps sebagai bagian dari upaya strategis untuk menjembatani kesenjangan talenta digital di Indonesia.

Tabel 1. 1 Proyeksi Kebutuhan Tenaga Kerja TIK Tahun 2022-2025

No	Nama Jabatan	Proyeksi Kebutuhan Tenaga Kerja			
		2022	2023	2024	2025
1	Network Operation Access	522.553	609.790	697.027	784.265
2	Network Operation Backbone	235.541	322.779	410.016	497.254
3	Software Engineer	109.047	129.111	148.304	162.262
4	Network Engineer	52.343	69.790	69.790	69.790
5	Software Architect	33.150	36.640	40.129	42.746
6	Network Assurance Specialist	30.533	30.533	30.533	30.533
7	Voice Communications Specialist	26.171	30.533	30.533	30.533
8	Telecommunication Technician/ Engineer	27.427	24.426	24.426	24.426
9	Data Analyst	31.406	36.640	42.746	51.470
10	Technical Project Specialist	21.809	39.257	56.704	65.428

Sumber: KEMNAKER. (2021). Satudata Kemnaker

Berbagai studi menunjukkan potensi DevSecOps dalam mempercepat proses pengembangan perangkat lunak sekaligus memperkuat aspek keamanan sistem, antara lain yang dilakukan oleh Akbar et al., 2022; Bedoya et al., 2024; Charoenwet et al., 2024; Garcia et al., n.d.; Wiedemann et al., 2023., namun temuan-temuan tersebut juga mengindikasikan masih adanya sejumlah kesenjangan yang perlu dijembatani, baik terkait pendekatan implementasi di tingkat organisasi, ketersediaan talenta yang kompeten, maupun desain program pelatihan yang sistematis dan kontekstual.

Pelatihan yang tersedia saat ini umumnya masih terfragmentasi berdasarkan bidang keahlian, seperti Pemrograman (*Programming*), Antar Muka (UI/UX), Rekayasa Perangkat Lunak (*Software Engineering*), Basis Data (*Database*), Jaringan (*Networking*), Arsitektur TI (IT *Architecture*), Keamanan (*Security*), dan Manajemen Proyek (*Project Management*). Setiap bidang pelatihan tersebut memerlukan waktu yang relatif panjang untuk dikuasai secara memadai. Sementara itu, laju perkembangan dan perubahan teknologi yang sangat cepat menuntut perusahaan untuk meningkatkan kompetensi SDM dalam waktu singkat, dengan orientasi pada kesiapan kerja (*job-ready*) yang selaras dengan kebutuhan dan konteks spesifik organisasi. Kondisi ini memperkuat perlunya rancangan pelatihan

yang terintegrasi, intensif, dan berorientasi praktik, seperti pendekatan bootcamp DevSecOps.

Kesenjangan inilah yang menegaskan urgensi penelitian ini untuk merancang sebuah model pelatihan DevSecOps berbasis *bootcamp* yang: (1) selaras dengan kebutuhan spesifik industri perbankan, (2) mengintegrasikan pendekatan pedagogis aktif yang telah terbukti efektif dalam meningkatkan keterlibatan dan capaian belajar, serta (3) didukung oleh instrumen evaluasi hasil belajar yang valid dan reliabel. Dengan demikian, penelitian ini diharapkan tidak hanya memberikan kontribusi teoretis bagi pengembangan model pelatihan DevSecOps, tetapi juga kontribusi praktis dalam mendukung transformasi digital sektor perbankan melalui peningkatan kompetensi talenta digital.

Dalam konteks pengembangan sumber daya manusia, pembelajaran, peningkatan kinerja, dan pelatihan merupakan tiga konsep yang saling berkaitan erat. Pembelajaran dipahami sebagai proses perolehan pengetahuan, keterampilan, dan sikap baru melalui pengalaman, instruksi, observasi, dan refleksi (Schunk, 2020), peningkatan kinerja merujuk pada upaya sistematis untuk menguatkan kapasitas individu maupun organisasi agar mampu mencapai tujuan strategis, yang dapat diwujudkan melalui berbagai intervensi, seperti pelatihan, pemberian umpan balik yang terstruktur, serta redesain proses kerja (Aguinis, 2023), sedangkan pelatihan adalah proses yang dirancang secara terstruktur untuk membekali pegawai dengan keterampilan spesifik yang diperlukan dalam pelaksanaan tugasnya, sehingga berkontribusi langsung terhadap peningkatan kinerja organisasi (Verhulst & DeCenzo, 2021). Pelatihan DevSecOps yang efektif seyogianya mampu mengintegrasikan ketiga konsep tersebut ke dalam suatu kerangka pembelajaran yang berorientasi praktik, kinerja, dan hasil (*performance- and outcome-based learning*).

Berdasarkan hasil wawancara awal dengan 15 responden yang terdiri atas 2 orang dengan pengalaman kerja lebih dari 3 tahun, 5 orang dengan pengalaman kerja 1–3 tahun, dan 8 orang *management trainee* TI perbankan yang merupakan *fresh graduate,* diperoleh data yang telah dianalisis oleh peneliti, dan hasilnya disajikan dalam tabel berikut:

Tabel 1. 2 Hasil Analisis Kebutuhan Awal

No	Pertanyaan	Tanggapan Responden
1	Pemahaman Terhadap DevSecOps	Empat responden memiliki pemahaman dasar DevSecOps, tiga responden sudah menerapkan sebagian praktik DevSecOps tetapi tanpa struktur, delapan responden belum memahami DevSecOps.
2	Penggunaan *tools* DevSecOps	Dua responden sudah menggunakan *tools* DevSecOps seperti Git, Jenkins, GitLab CI, Jira, atau Trello, empat responden mengetahui namun belum pernah menggunakan, dan sembilan responden belum mengetahui tentang *tools* DevSecOps.
3	Urgensi Pelatihan	Dua belas responden menyatakan bahwa pelatihan sangat diperlukan, dua responden merasa pelatihan ini penting namun bukan prioritas, dan satu responden merasa cukup dengan sumber belajar mandiri.
4	Metode Pelatihan yang Dianggap Efektif	Sembilan responden memilih *Bootcamp* karena intensif dan terstruktur, empat responden memilih metode *e-learning* untuk fleksibilitas, dan dua responden memilih metode pelatihan konvensional (*classroom*).
5	Hambatan Mengadopsi DevSecOps	Tujuh responden menyebut kurangnya keterampilan teknis di tim, lima responden mengkhawatirkan biaya implementasi, dan tiga responden tidak memiliki waktu untuk pelatihan.

Berdasarkan tabel di atas, *bootcamp* yang dirancang sesuai kebutuhan industri, berfokus pada keterampilan dan dapat dilaksanakan secara sinkron (*live online*) maupun asinkron (*self-paced online*) adalah yang paling dibutuhkan. Hasil ini sesuai dengan penelitian Berridge, Jain, dan Biyani yang menyimpulkan bahwa pendekatan *bootcamp* terbukti efektif dalam membekali peserta dengan keterampilan praktis dalam waktu singkat (Berridge et al., 2020), sehingga sesuai dengan tuntutan industri perbankan yang membutuhkan tenaga kerja siap pakai. Oleh karena itu, pengembangan model pelatihan DevSecOps berbasis bootcamp menjadi sebuah kebutuhan yang cocok untuk menjawab kesenjangan yang ada.

B. Batasan Penelitian

Berdasarkan uraian pada latar belakang maka penelitian ini dibatasi pada perancangan, pengembangan, dan evaluasi model pelatihan yang:

1. Penelitian ini dilakukan di institusi perbankan.
2. Ditujukan untuk *digital talent/ management trainee* Perbankan.
3. Model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* dirancang sebagai panduan bagi *digital talent/ management trainee* untuk meningkatkan pengetahuan dan keterampilan dalam penerapan DevSecOps, sehingga mereka dapat secara efektif membangun, mengoperasikan, dan memecahkan permasalahan keamanan yang dihadapi dalam Teknologi Informasi (TI) di institusi perbankan.

C. Rumusan Masalah

Rumusan masalah penelitan disertasi ini adalah:

1. Bagaimana mengembangkan model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan?
2. Bagaimana kelayakan model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan?
3. Bagaimana efektivitas model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan?

D. Tujuan Penelitian

Penelitian ini memiliki tujuan yaitu:

1. Menghasilkan model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan.
2. Menganalisis kelayakan model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan.
3. Menganalisis efektivitas model pelatihan DevSecOps menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan.

E. Signifikansi Penelitian

Penelitian dan pengembangan model pelatihan *DevSecOps* menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan, untuk meningkatkan pengetahuan dan keterampilan dalam penerapan DevSecOps, sehingga mereka dapat secara efektif membangun, mengoperasikan, dan

memecahkan permasalahan keamanan yang dihadapi dalam Teknologi Informasi (TI) di institusi perbankan.

Hasil penelitian ini diharapkan juga dapat memberikan manfaat dan signifikansi antara lain:

1. Model pelatihan *DevSecOps* menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan perlu dikembangkan agar dapat menunjang kinerja TI di institusi perbankan.
2. Tambahan literatur bagi praktisi dan akademisi tentang model pelatihan yang sesuai untuk pelatihan *DevSecOps* menggunakan pendekatan *Bootcamp* pada *digital talent/ management trainee* perbankan.
3. Model pelatihan yang sesuai untuk pelatihan *DevSecOps* menggunakan pendekatan *Bootcamp* diharapkan dapat membuat pelatihan yang lebih fokus, intensif, personal, dan kolaboratif dengan waktu yang lebih singkat.

F. Kebaruan Penelitian (*State of the Art*)

Bootcamp adalah model pelatihan intensif yang fokus pada pengajaran keterampilan praktis dalam waktu singkat. Namun, penelitian tentang penerapan model *Bootcamp* dalam pelatihan DevSecOps masih terbatas.

Peneliti melakukan tinjauan dan analisis literatur terhadap penelitian dan pengembangan yang membahas tentang pelatihan DevSecOps dan pendekatan *bootcamp* dalam pelatihan untuk membandingkan dengan penelitian yang sedang dilakukan. Tujuannya adalah agar mendapatkan kebaruan penelitian yang sedang dilakukan (*State of The Art*).

Tabel 1. 3 Penelitian yang Relevan

No	Tahun	Penulis dan Sumber	Hasil Penelitian
1	2023	Fernandez-Gauna, B., Rojo, N., & Graña, M. *Automatic Feedback and Assessment of Team-Coding Assignments in a DevOps Context.* International Journal of Educational Technology in Higher Education, 20.	Penelitian ini menghasilkan proses penilaian otomatis untuk tugas pengkodean tim. Metode ini mendefinisikan beberapa Metrik Kinerja Tim untuk mengukur properti perangkat lunak yang dikembangkan oleh masing-masing tim, dan juga penggunaan teknik DevOps yang benar. Penilaian ini melacak kemajuan pada masing-masing metrik oleh

No	Tahun	Penulis dan Sumber	Hasil Penelitian
			masing-masing kelompok, dan juga menentukan Metrik Kinerja Individu untuk mendistribusikan kredit di antara anggota tim atas setiap perubahan dalam Metrik Kinerja Tim.
2	2023	Tanzil, M. H., Sarker, M., Uddin, G., & Iqbal, A. *A mixed method study of DevOps challenges*. Information and Software Technology, 161, 107244. https://doi.org/10.1016/j.infsof.2023.107244	Adanya kebutuhan akan dokumentasi dan sumber pembelajaran yang lebih baik untuk mempelajari alat dan teknik DevOps yang berubah dengan cepat bagi pengembang perangkat lunak (*software developers*)
3	2023	Wiedemann, A., Wiesche, M., Gewald, H., & Krcmar, H. *Integrating development and operations teams: A control approach for DevOps.* Information and Organization, 33(3), 100474. https://doi.org/10.1016/j.infoandorg.2023.100474	Penelitian ini memberikan wawasan tentang area kendali (*area of* control) yang terabaikan dalam tim lintas fungsi dan menjelaskan sifat dinamis dan berulang dari kendali tim DevOps. Peneliti memperoleh tiga dimensi gabungan yaitu: a. partisipasi dalam visi bersama (*participation in a shared vision*), b. hak untuk menentukan nasib bersama (*right of co-determination*), dan c. akal sehat (*common sense of duty*) dalam menjalankan tugas untuk mengendalikan tim DevOps yang dapat digunakan untuk mengatasi ketegangan dalam tim.
4	2022	Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. *Challenges and solutions when adopting* DevSecOps*: A systematic review.* Information and Software Technology, 141, 106700. https://doi.org/10.1016/j.infsof.2021.106700	Peneliti melakukan tinjauan sistematis tentang tantangan dan solusi dalam mengadopsi DevSecOps, menyoroti kebutuhan akan pendidikan dan pelatihan yang memadai
5	2019	Rahman, A., Mahdavi-Hezaveh, R., & Williams, L. *Where Are the Gaps? A Systematic Mapping Study*	Peneliti menyelidiki praktik DevSecOps di industri, mengidentifikasi tantangan seperti

No	Tahun	Penulis dan Sumber	Hasil Penelitian
		of Infrastructure as Code Research. Information and Software Technology, 108, 65–77. https://doi.org/10.1016/j.infsof.2018.12.004	kurangnya kesadaran dan keterampilan yang memadai.
6	2019	Luz, W. P., Pinto, G., & Bonifácio, R. *Adopting DevOps in the real world: A theory, a model, and a case study.* Journal of Systems and Software, 157, 110384. https://doi.org/10.1016/j.jss.2019.07.083	Hasil penelitian menemukan bahwa adopsi DevOps melibatkan hubungan yang sangat spesifik antara tujuh kategori: kelincahan (*agility*), otomatisasi (*automation*), budaya kolaboratif (*collaborative culture*), pengukuran berkelanjutan (*continuous measurement*), jaminan kualitas (*quality assurance*), ketahanan (*resilience*), berbagi (*sharing*), dan transparansi (*transparency*).
7	2024	Monica, P., & Jen, A. *The influence of intensive clinical skills '**bootcamps**' on nursing students' perceptions of ability to provide acute care: A mixed methods study.* Nurse Education Today, 134, 106099. https://doi.org/10.1016/j.nedt.2024.106099	Penelitian yang dilakukan untuk menguji pengaruh *Bootcamp* keterampilan klinis intensif terhadap persepsi siswa dalam memberikan perawatan dalam situasi akut. Hasil penelitian menyatakan bahwa pelatihan intensif keterampilan klinis (*intensive clinical skills bootcamps*) mengembangkan kepercayaan diri yang dirasakan oleh peserta didik dengan memberikan umpan balik dan kesempatan untuk refleksi guna membangun koneksi. Kesempatan bagi peserta didik untuk merefleksikan kompetensi mereka saat ini mendukung pengembangan wawasan yang realistis terhadap kemampuan yang dipersepsikan.
8	2023	Qadriani, F. E., & Windasari, N. A. ***Battle of Bootcamp**: Analyzing Factor Affecting Customer Satisfaction and*	Penelitian ini bertujuan untuk mengeksplorasi faktor-faktor penentu kepuasan siswa pada platform Coding *Bootcamp* di Indonesia. Motivasi tidak

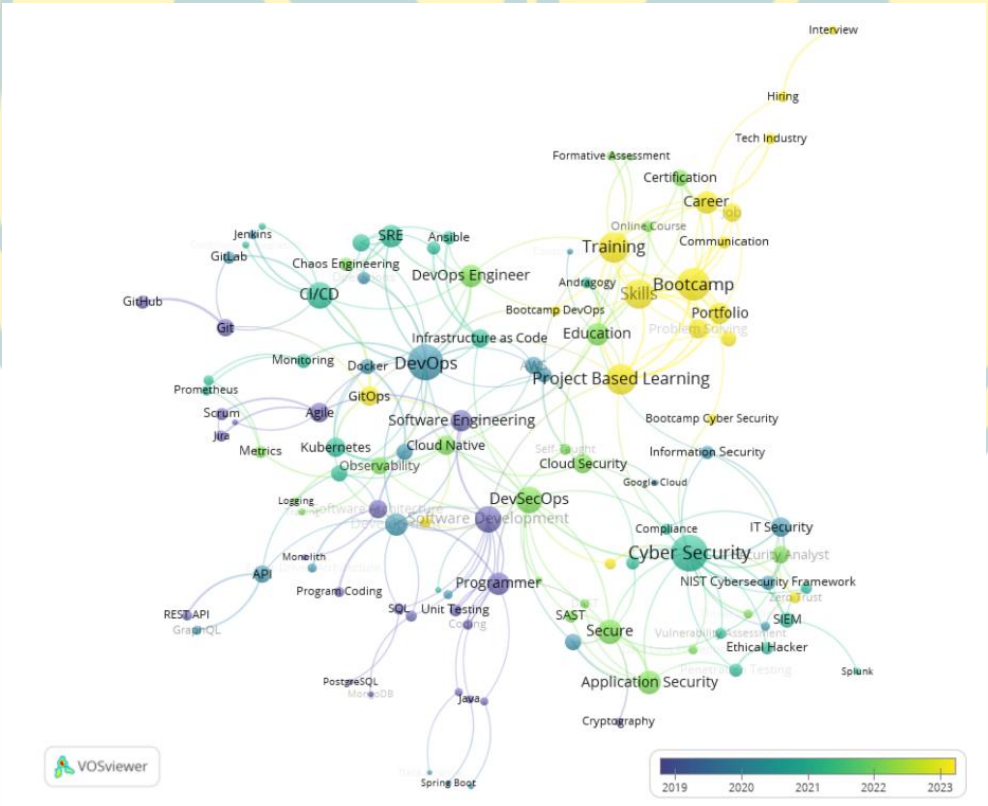
No	Tahun	Penulis dan Sumber	Hasil Penelitian
		Continuance Intention in Coding Bootcamp Industry Indonesia. International Journal of Current Science Research and Review, 06(01). https://doi.org/10.47191/ijcsrr/V6-i1-06	ditemukan menjadi variabel yang signifikan dalam penelitian ini. Namun model *Bootcamp* berpotensi mengganggu (*disrupt*) pendidikan tinggi dan secara mendasar mengubah sifat pendidikan dan pelatihan jika berhasil memenuhi kebutuhan pelanggan.
9	2022	Lang, G., & Sharp, J. H. *Coding Bootcamp Satisfaction: A Research Model and Survey Instrument.* Information Systems Education Journal, 20(2), 49–60.	Terdapat empat belas faktor kepuasan peserta didik yang diidentifikasi pada penelitian ini, yaitu: Kualitas Pengajar (*Quality of Instructors*), Nilai Mentor (*Value of Mentors*), Ketersediaan Asisten Pengajar (*Availability of TA*), Akses ke Staf Pendukung (*Access to Support Staff*), Provisi Layanan Pelanggan (*Provision of Customer Service*), Ketatnya Kurikulum (*Rigor of Curriculum*), Ketepatan Pedagogi (*Appropriateness of Pedagogy*), Pengembangan Hubungan Peer (*Development of Peer Connections*), Atmosfir yang Kondusif (*Conduciveness of Atmosphere*), Penggunaan Teknologi yang Tepat (*Use of Appropriate Technology*), Keterjangkauan (*Affordability*), Keterbukaan Informasi (*Openness of Information*), Kualitas Materi Persiapan (*Quality of Prep Course*), Level dari Support Setelah *Bootcamp* (*Level of Post-Bootcamp Support*)
10	2022	Goger, A., Parco, A., & Vegas, E. *Learning and Working in the Digital Age: Advancing Opportunities and Identifying the Risks.* Brookings Institution.	Penelitian ini bertujuan untuk membantu para pengambil keputusan memahami sifat dari perubahan-perubahan dalam teknologi pendidikan dan perekrutan, serta kebutuhan mendesak untuk membangun kerangka tata kelola yang

No	Tahun	Penulis dan Sumber	Hasil Penelitian
			mendukung akses yang setara, mengurangi keraguan, dan melindungi dari eksploitasi dan penyalahgunaan.
11	2020	Berridge, C., Jain, S., & Biyani, C. S. *Defining boot camp: A supporting literature review.* South-East Asian Journal of Medical Education, 13(2), 3. https://doi.org/10.4038/seajme.v13i2.204	*Bootcamp* pendidikan kedokteran (*medical education bootcamps*) telah terbukti menjadi pelatihan yang efektif untuk meningkatkan keterampilan dan kepercayaan diri, meskipun definisi tentang apa itu *bootcamp* dan bagaimana perbedaannya dengan pelatihan lain masih belum jelas.
12	2019	Price, R., & Dunagan, A. *Betting on Bootcamps: How Short-Course Training Programs Could Change the Landscape of Higher Ed.* Clayton Christensen Institute for Disruptive Innovation.	Untuk berhasil memasuki industri dan konteks pelatihan baru, *Bootcamp* harus terus berinovasi. Namun jika tantangan inovasi tersebut berhasil diatasi, model *Bootcamp* dapat mengganggu (*disrupt*) dan mengubah lanskap pendidikan dan pelatihan secara dramatis dan permanen.
13	2022	Berge, Z. L. *Designing Workplace Training for Generational Differences: Does IT Matter?* Merits, 2(4), Article 4. https://doi.org/10.3390/merits2040028	Desainer Pembelajaran harus mencari tahu sebanyak mungkin karakteristik dan preferensi peserta didik yang terlibat, seperti pengalaman, tahap karir, usia, sikap, kebiasaan kerja, motivasi, budaya, dll. Jangan berfokus pada perbedaan generasi, namun desainer pembelajaran harus fleksibel untuk memenuhi kebutuhan seluruh karyawan di semua kelompok umur.

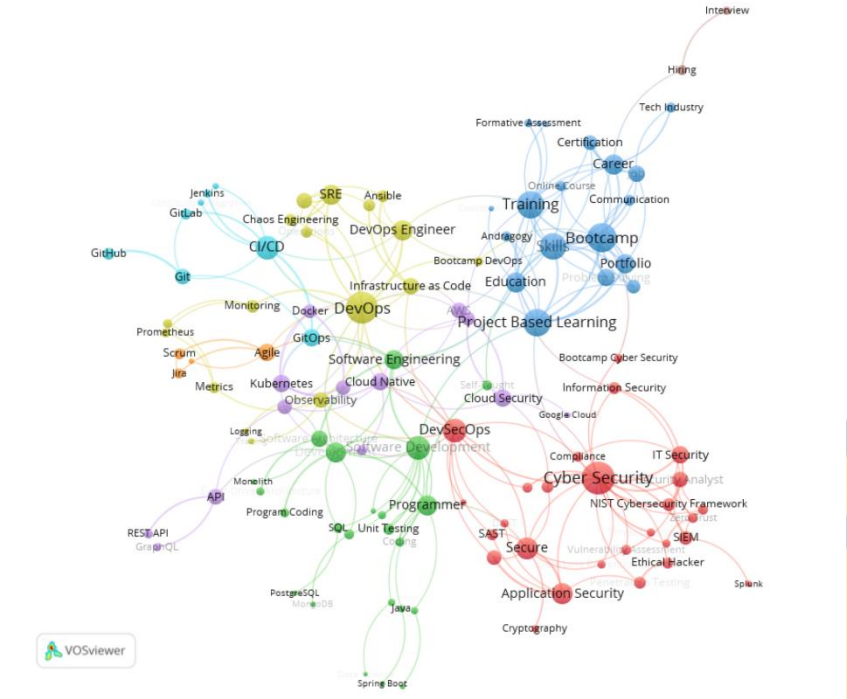
Berdasarkan tinjauan terhadap 13 jurnal relevan dan diperkuat oleh hasil analisis bibliometrik, dapat ditarik kesimpulan bahwa DevSecOps telah diakui secara luas sebagai pendekatan yang sangat efektif untuk mempercepat siklus rilis sekaligus meningkatkan postur keamanan dalam pengembangan perangkat lunak. Namun, efektivitas penerapannya di industri sangat bergantung pada kesiapan

talenta yang memiliki kompetensi yang tepat. Di sinilah celah penelitian yang krusial teridentifikasi: dari seluruh artikel referensi, belum ditemukan adanya pembahasan yang secara spesifik merumuskan sebuah model pelatihan DevSecOps yang terstruktur dan teruji. Oleh karena itu, penelitian ini menjadi penting karena berfokus untuk merancang sebuah model pelatihan yang efektif melalui pendekatan bootcamp, guna menjembatani kesenjangan antara kebutuhan industri akan praktik DevSecOps dan minimnya panduan implementasi pelatihannya.

Tinjauan literatur ini menegaskan pentingnya DevSecOps dalam pengembangan perangkat lunak modern dan kebutuhan akan pelatihan yang efektif. Metode pelatihan konvensional yang ada saat ini membutuhkan waktu yang cukup lama untuk dapat mencetak tenaga ahli DevSecOps. Untuk itu dibutuhkan metode pelatihan baru dengan pendekatan *bootcamp* yang lebih efisien dan efektif, terutama dari sisi waktu pelatihan.



Gambar 1. 2 Visualisasi Keterhubungan Variabel



Gambar 1. 3 Visualisasi Kepadatan Kata Kunci Kejadian Bersama (*Co-Occurence*)

Berdasarkan hasil analisis bibliometrik menunjukkan bahwa DevSecOps berkaitan erat dengan *Cyber Security*, *Software Engineering*, dan *DevOps* yang merupakan isu penting dalam pengembangan aplikasi saat ini. Peta bibliometrik juga mengindikasikan keterkaitan erat antara pendekatan *Bootcamp* dengan *Project Based Learning*, yang dalam konteks teknologi pendidikan berperan sebagai strategi pedagogis untuk meningkatkan efektivitas, efisiensi, dan keterlibatan belajar peserta didik melalui integrasi antara prinsip-prinsip pedagogi dan teknologi digital. Oleh karena itu, pengembangan model pelatihan DevSecOps dengan pendekatan *bootcamp* tidak hanya relevan, tetapi juga strategis sebagai jawaban atas tantangan integrasi keamanan dan pembelajaran berbasis keterampilan dalam era digital.

Meskipun penelitian-penelitian yang ada telah menyelidiki berbagai aspek *Bootcamp*, termasuk desain, efektivitas, hasil, dan pengalaman peserta, namun penelitian yang secara khusus meneliti penerapan metode *Bootcamp* dalam konteks pelatihan DevSecOps terutama untuk *digital talent/ management trainee* perbankan masih belum ada. Oleh karena itu, diperlukan penelitian lebih lanjut untuk mengembangkan model pelatihan DevSecOps menggunakan pendekatan

Bootcamp, yang mempertimbangkan praktik-praktik terbaik (*best practices*), konten pelatihan, strategi pengajaran, dan evaluasi hasil pelatihan.

Penelitian ini akan berkontribusi pada kemajuan bidang tersebut dengan memberikan kerangka kerja yang kuat untuk pelatihan DevSecOps, membantu mengatasi kesenjangan keterampilan, dan mendorong adopsi praktik keamanan yang lebih baik dalam pengembangan perangkat lunak.