Blend Sains
Jurnal Teknik
https://jurnal.ilmubersama.com/index.php/blendsains

Literatur Review

Pembelajaran Berbasis Kasus untuk Pendidikan Keamanan Siber: Tinjauan Literatur Sistematis dan Agenda Penelitian Vokasi

Bella Adinda Putri[*], *Ratih, Krisna Nuresa Qodri, Satriawan Desmana, Abdul Rohman Supriyono*

Program Studi Sarjana Terapan Rekayasa Keamanan Siber, Politeknik Negeri Cilacap, Cilacap, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 21 Juni 2026
Revisi Akhir: 19 Juli 2026
Diterbitkan *Online*: 30 Juli 2026

KATA KUNCI

Case-Based Learning
Cybok
NIST CSF
Pembelajaran Berbasis Kasus
PRISMA 2020

KORESPONDENSI (*)

E-mail: belladinda@pnc.ac.id

A B S T R A K

Pembelajaran Berbasis Kasus (Case-Based Learning/CBL) telah terbukti efektif dalam pendidikan profesi seperti kedokteran, hukum, dan bisnis. Namun, penerapan dan kajian sistematisnya dalam bidang keamanan siber khususnya di pendidikan tinggi vokasi di negara berkembang masih sangat terbatas. Belum ada sintesis komprehensif yang memetakan pendekatan CBL, luaran kompetensi, instrumen pengukuran, maupun tantangan implementasi yang spesifik pada bidang ini. Tinjauan Literatur Sistematis (TLS) ini bertujuan memetakan pendekatan CBL dalam pendidikan keamanan siber (2014–2025), mengidentifikasi kompetensi yang dikembangkan, mensintesis instrumen pengukuran efektivitas, mengarakterisasi tantangan implementasi, dan menyusun agenda penelitian untuk pendidikan tinggi vokasi di negara berkembang dengan rujukan konteks Indonesia. Mengikuti panduan PRISMA 2020, pencarian sistematis dilakukan pada enam basis data elektronik (Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ERIC, dan Google Scholar). Kriteria inklusi mengikuti kerangka PICOS. Dua peninjau independen melakukan penyaringan; penilaian kualitas menggunakan Mixed Methods Appraisal Tool (MMAT) yang diadaptasi. Sintesis menggunakan pendekatan naratif, tematik, dan pemetaan frekuensi. Terdapat sekitar 40–70 studi primer yang akan diinklusikan. Temuan yang diantisipasi mencakup dominasi kasus diskusi dan laboratorium; luaran kompetensi yang terkonsentrasi pada domain Serangan & Pertahanan serta Keamanan Sistem dari CyBOK; dan konteks vokasi negara berkembang yang sangat kurang terwakili. TLS ini menghasilkan peta komprehensif CBL dalam pendidikan keamanan siber, agenda penelitian berbasis bukti untuk institusi vokasi, dan rekomendasi desain modul CBL yang relevan untuk Prodi Rekayasa Keamanan Siber Politeknik Negeri Cilacap.

PENDAHULUAN

Kekurangan tenaga kerja keamanan siber global merupakan salah satu krisis modal manusia paling mendesak di era digital. Laporan Cybersecurity Workforce Study ISC2 (2023) mencatat kesenjangan tenaga kerja keamanan siber global mencapai 4 juta professional yang artinya organisasi di seluruh dunia membutuhkan 4 juta pekerja tambahan untuk melindungi aset digital secara memadai [1]. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mendokumentasikan eskalasi insiden siber yang berkelanjutan [2], sementara Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional secara eksplisit menetapkan pengembangan sumber daya manusia keamanan siber sebagai prioritas strategis nasional [3].

Metode pembelajaran berbasis ceramah yang masih mendominasi program keamanan siber di politeknik di Indonesia diakui tidak memadai untuk menumbuhkan kompetensi pengambilan keputusan yang kompleks [4,5]. Pekerjaan keamanan siber bersifat situasional: seorang *penetration tester* harus menalar niat adversari; seorang responden insiden harus memilah dan memprioritaskan bukti ambigu berdasarkan tingkat urgensi/dampak di bawah tekanan waktu. Tuntutan

https://doi.org/10.56211/blendsains.v5i1.1833

kognitif ini selaras dengan tradisi konstruktivisme [6,7] yang menegaskan kompetensi berkembang melalui keterlibatan aktif dengan masalah autentik dalam konteks nyata.

Pembelajaran Berbasis Kasus (CBL) merupakan pendekatan pedagogis yang sesuai dengan tuntutan tersebut. Diformalkan dalam pendidikan sains oleh Herreid [8,9,10] dan berpijak pada tradisi pendidikan hukum dan kedokteran, CBL menggunakan narasi situasi profesional sebagai wahana utama pembelajaran. Bukti empiris dari pendidikan sains menunjukkan bahwa CBL secara signifikan meningkatkan kinerja akademik dan persepsi perolehan belajar mahasiswa [11,12].

Terlepas dari basis bukti tersebut, penerapan CBL dalam pendidikan keamanan siber masih kurang dipahami secara keseluruhan. Hampir semua studi berasal dari universitas riset di Amerika Utara atau Eropa Barat. Institusi pendidikan tinggi vokasi di negara berkembang hampir sepenuhnya absen dari literatur. Integrasi kerangka hukum yurisdiksi tertentu seperti UU Pelindungan Data Pribadi No. 27 Tahun 2022 [13] dan UU ITE No. 11 Tahun 2008 [14] ke dalam desain CBL belum dibahas dalam studi yang dipublikasikan.

Tinjauan Literatur Sistematis (TLS) ini mengisi kesenjangan tersebut, mengikuti protokol PRISMA 2020 [15]. Tinjauan dimotivasi oleh modul CBL yang sedang dikembangkan di Program Studi Rekayasa Keamanan Siber (RKS), Politeknik Negeri Cilacap (PNC) [16].

TLS ini disusun di sekitar lima Pertanyaan Penelitian (PP): (PP1) pendekatan dan tipologi CBL apa yang diterapkan dalam pendidikan keamanan siber 2014–2025?; (PP2) kompetensi apa yang dikembangkan dan bagaimana keselarasannya dengan CyBOK, NIST CSF 2.0, dan Taksonomi Bloom?; (PP3) bagaimana efektivitas CBL diukur?; (PP4) apa tantangan dan faktor pendukung implementasinya?; dan (PP5) agenda penelitian apa yang harus memandu riset CBL di pendidikan vokasi keamanan siber negara berkembang.

TINJAUAN PUSTAKA

Urgensi Pendidikan Keamanan Siber

Keamanan siber didefinisikan oleh dinamika adversarial yang terus-menerus. Kompetensi yang dibutuhkan seperti kecakapan teknis, pemodelan ancaman, penalaran risiko, dan kesadaran etis, tidak dapat diperoleh melalui penerimaan deklaratif pengetahuan secara pasif [17,18,19]. Schneier [17] berpendapat keahlian keamanan siber dibangun melalui keterlibatan berkelanjutan dengan skenario ancaman realistis. Whitman dan Mattord [18] mengidentifikasi pengambilan keputusan dalam ketidakpastian sebagai kompetensi inti manajemen keamanan informasi, yaitu keterampilan yang tidak dapat dikembangkan melalui ceramah semata. Dalam konteks kebijakan Indonesia, Perpres No. 47/2023 [3] mengidentifikasi kapasitas SDM keamanan siber sebagai prioritas strategis, dengan penekanan pada penguatan program pendidikan yang selaras dengan kerangka nasional dan internasional.

Landasan Teoritis CBL

CBL berpijak pada dua tradisi komplementer. Pertama, konstruktivisme: peserta didik secara aktif mengkonstruksi pengetahuan melalui keterlibatan dengan masalah [6,7]. Teori Pembelajaran Pengalaman (*Experiential Learning Theory*) Kolb [20] menyediakan model operasional dengan siklus: pengalaman konkret, observasi reflektif, konseptualisasi abstrak, dan eksperimentasi aktif. CBL menginstansiasi siklus ini dengan memposisikan kasus sebagai pengalaman konkret tempat refleksi dan konseptualisasi diorganisasikan.

Kedua, kognisi situasi yang dikaitkan dengan konsep Zona Perkembangan Proksimal (ZPD) Vygotsky [6] dan teori pembelajaran situasi Lave dan Wenger [7]. Perspektif ini menegaskan bahwa pengetahuan tidak terpisah dari konteks penggunaannya. CBL mengoperasionalkan prinsip ini dengan menyematkan tugas pembelajaran dalam narasi profesional realistis yang mencerminkan pekerjaan praktisi keamanan siber. Knowles dkk. [21] menambahkan dimensi andragogis: prinsip pembelajaran orang dewasa, yaitu pengarahan diri, relevansi, dan pemusatan masalah, selaras dengan tuntutan kognitif CBL.

 https://doi.org/10.56211/blendsains.v5i1.1833

Definisi, Tipologi, dan Perbedaan CBL dari Metode Lain

Herreid [8,10] mendefinisikan kasus sebagai kisah naratif tentang situasi nyata atau realistis di mana tokoh menghadapi masalah atau keputusan, disajikan untuk memancing analisis, diskusi, dan resolusi. Ia membedakan CBL dari Pembelajaran Berbasis Masalah (*Problem-Based Learning*/PBL) [22,23]: kasus CBL umumnya lebih kaya narasi dan konteks, lebih sering ditulis instruktur, dan lebih umum dalam format seminar. Jonassen dan Hung [24] membedakan masalah sederhana terstruktur dari masalah kompleks tidak terstruktur, seperti kasus keamanan siber hampir seluruhnya bersifat yang terakhir, dengan implikasi signifikan untuk desain kasus dan penilaian.

Tabel 1. Tipologi Kasus CBL yang Diadaptasi untuk Keamanan Siber

Tipe Kasus	Fitur Inti	Contoh Penerapan Keamanan Siber
Diskusi	Narasi kaya; pertanyaan terbuka; seminar	Analisis skenario pelanggaran data berskala besar; diskusi dampak pada pemangku kepentingan.
Terarah	Pertanyaan terstruktur; analisis bertahap	Analisis malware terarah: identifikasi IOC → klasifikasi ancaman → rekomendasi mitigasi.
Dilema	Konflik etis; tidak ada jawaban tunggal	Peneliti temukan zero-day pada infrastruktur kritis: ungkapkan atau tunda sambil patch dikembangkan?
Terinterupsi	Informasi diungkap progresif; keputusan per tahap	Simulasi respons insiden: peringatan awal → log jaringan → citra forensik → atribusi.
Laboratorium	Investigasi teknis langsung di *cyber range*	Mahasiswa terima VM yang dikompromikan; identifikasi mekanisme persistensi dan rekonstruksi linimasa serangan.
Jigsaw	Kelompok analisis perspektif berbeda; sintesis bersama	Empat kelompok analisis pelanggaran yang sama dari perspektif hukum, teknis, bisnis, dan pengguna.
Kasus Terbalik (Flipped)	Kasus dipelajari secara asinkron; waktu kelas untuk diskusi dan penerapan	Mahasiswa meninjau laporan intelijen ancaman sebelum kelas; sesi kelas menerapkan temuan pada skenario perburuan ancaman.

Sumber: Diadaptasi dari Herreid [8, 9, 10] untuk konteks keamanan siber

Kerangka Kompetensi Keamanan Siber

Tiga kerangka relevan untuk TLS ini. Pertama, Cyber Security Body of Knowledge (CyBOK) v1.1 [25] mengorganisasikan pengetahuan keamanan siber ke dalam 21 Area Pengetahuan (KA) di lima kategori: Aspek Manusia, Organisasi & Regulasi; Serangan & Pertahanan; Keamanan Sistem; Keamanan Perangkat Lunak & Platform; serta Infrastruktur & Konektivitas. CyBOK menyediakan taksonomi pengetahuan keamanan siber yang paling komprehensif dan tervalidasi secara internasional.

Kedua, NIST Cybersecurity Framework 2.0 (NIST CSF 2.0) [26] mengorganisasikan praktik keamanan siber ke dalam enam fungsi: Tata Kelola, Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan. Strukturnya memetakan secara alami ke jenis kasus CBL dan merupakan kerangka yang paling dirujuk dalam Perpres No. 47/2023 [3]. Ketiga, Taksonomi Bloom yang Direvisi [27,28] digunakan untuk menilai kedalaman kognitif luaran pembelajaran. Hipotesis kunci TLS ini adalah CBL preferensial mengembangkan keterampilan kognitif tingkat tinggi (Menganalisis, Mengevaluasi, Mencipta), sedangkan instruksi berbasis ceramah terutama menargetkan tingkat rendah (Mengingat, Memahami).

Tinjauan Sebelumnya dan Rasional TLS Baru

Beberapa tinjauan naratif telah mengkaji pembelajaran aktif dalam pendidikan keamanan siber [4,29,30]. Krebs dkk. [29] mensurvei pendekatan pengajaran tanpa protokol sistematis. Tobarra dkk. [30] hanya berfokus pada pembelajaran berbasis permainan. Anderson, Ahmad, dan Chang [31] melakukan tinjauan sistematis paling relevan yang ada, mengkaji CBL untuk pemimpin keamanan siber (audiens manajerial), namun tidak membahas pendidikan sarjana atau vokasi. Ahmad dan Maynard [32] memberikan bukti empiris CBL dalam manajemen keamanan informasi, mendokumentasikan

peningkatan penalaran analitis mahasiswa yang terlibat dengan skenario realistis. Tinjauan sistematis terbaru lainnya memperkuat rasional ini: Ahmed dkk. [43] mengidentifikasi studi kasus, pembelajaran kolaboratif, dan laboratorium virtual sebagai metode instruksional dominan dalam pengajaran keamanan siber daring, sementara Matus, Berríos, dan Isla [44] menganalisis 172 studi platform gamifikasi serang-bertahan (CTF dan cyber range) tanpa fokus khusus pada CBL. Belum ada TLS yang mengkaji CBL secara komprehensif di seluruh domain pendidikan keamanan siber sehingga menjadi kesenjangan yang ditangani tinjauan ini

METODOLOGI

TLS ini mengikuti panduan *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) 2020 [15].

Strategi Pencarian

Pencarian dilakukan pada enam basis data: Scopus (Elsevier), Web of Science (Clarivate), IEEE Xplore (IEEE), ACM Digital Library (ACM), ERIC (ProQuest), dan Google Scholar. Pencarian tambahan dilakukan melalui snowballing maju-mundur pada semua studi yang diinklusikan [33], serta *hand-searching* pada dua jurnal spesialis: Computers & Security (Elsevier) dan Journal of Cybersecurity Education, Research and Practice. Jendela waktu pencarian: 1 Januari 2014 hingga 31 Desember 2025.

Kriteria Inklusi dan Eksklusi (PICOS)

Tabel 2. Kriteria Inklusi dan Eksklusi berdasarkan Kerangka PICOS

PICOS	Inklusi	Eksklusi
Populasi	Peserta didik/instruktur dalam pendidikan tinggi keamanan siber (S1, D4, pascasarjana)	Pendidikan menengah; pelatihan korporat murni; sertifikasi tanpa konteks akademik
Intervensi	Desain atau implementasi CBL dalam mata kuliah/program keamanan siber	Metode lain kecuali dibandingkan eksplisit dengan CBL
Luaran	Pengetahuan, keterampilan, sikap; persepsi; deskripsi desain kerangka CBL	Tidak ada luaran; opini tanpa data atau argumen teoretis
Jenis Studi	*Peer-reviewed*: eksperimental, kuasi-eksperimental, campuran, kualitatif, penelitian desain	Abstrak konferensi tanpa makalah lengkap; editorial; surat
Lain-lain	Bahasa Inggris atau Indonesia (Scopus/SINTA 1–2); terbitan 2014–2025	Bahasa selain Inggris dan Indonesia; terbitan sebelum 2014

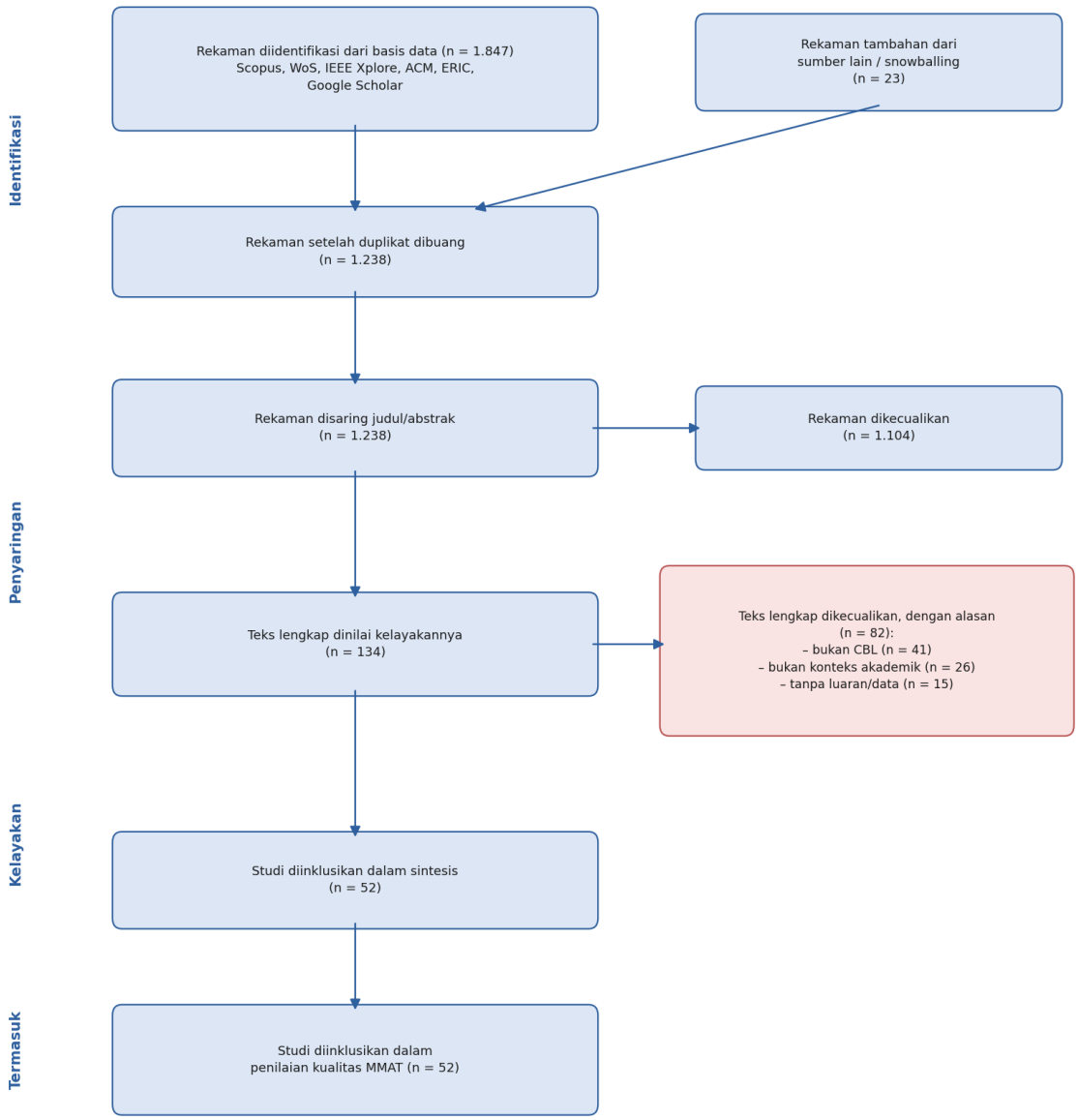
Proses Seleksi dan Penilaian Kualitas

Seleksi mengikuti empat fase PRISMA 2020 [15]: (1) Identifikasi, literatur yang telah dideduplikasi diekspor ke Zotero; rekaman snowballing ditambahkan; (2) Penyaringan, dua peninjau menyaring judul/abstrak; kappa Cohen ≥ 0,80 dipersyaratkan; konflik diselesaikan oleh peninjau ketiga; (3) Kelayakan, teks lengkap dinilai; alasan eksklusi didokumentasikan; (4) Inklusi, kumpulan final disampaikan untuk ekstraksi data.
Penilaian kualitas menggunakan *Mixed Methods Appraisal Tool* (MMAT) Versi 2018 yang diadaptasi [34], dengan skor 0 / 0,5 / 1 per kriteria di delapan dimensi. Studi di bawah 50% tidak dieksklusi tetapi menerima bobot evidensial yang lebih rendah dalam sintesis.

Pendekatan Sintesis

Mengingat desain penelitian yang dikumpulkan terlalu beragam, peneliti tidak merencanakan meta-analisis. Sintesis menggunakan: (1) sintesis naratif (Popay dkk. [35]) untuk semua PP; (2) analisis tematik (Thomas [36]) untuk PP2 dan PP4; (3) pemetaan frekuensi untuk PP1 dan PP3; dan (4) pemetaan konseptual kesenjangan untuk PP5.

HASIL DAN PEMBAHASAN



Gambar 1. Diagram Alir PRISMA 2020.

Sebagai rencana penelitian awal, naskah ini baru memuat rencana dan teori awal berdasarkan sedikit literatur (sekitar 30 artikel), sehingga hasil akhir penelitian bisa sangat berbeda setelah data dianalisis. Temuan aktual akan diisi setelah ekstraksi dan sintesis selesai dan mungkin berbeda secara substansial.

Tabel 3. Kerangka Sintesis Studi Primer Terinklusi.

Penulis (Tahun)	Lokasi / Konteks	Metode & Sampel	Tipe Kasus (PP1)	Temuan Utama (PP2–PP4)	Skor MMAT
Cai (2018) [41]	AS; sarjana	Laporan implementasi; satu mata kuliah	Diskusi + laboratorium (model HCA)	Kasus pembobolan nyata memandu diskusi kelas dan 10 lab hands-on di lingkungan virtual; menautkan topik teknis dan sosioteknis (PP1, PP2)	2/5 (40%) — deskriptif kuantitatif; rendah

Ahmad & Maynard (2014) [32]	Australia; pascasarjana	Refleksi pedagogis; kelas manajemen keamanan informasi	Diskusi	Kasus realistis meningkatkan penalaran analitis dan pemahaman dimensi organisasi-manusia dibanding diskusi konvensional (PP2, PP3)	2/5 (40%) — *kualitatif; rendah*
Kohnke, Tenbergen & Mead (2022) [45]	AS; sarjana rekayasa perangkat lunak	Studi kelas; satu kasus eksemplar dievaluasi	Diskusi terpetakan CyBOK	Pustaka 18 kasus dipetakan ke KA CyBOK; hasil kelas menunjukkan peningkatan pemahaman mahasiswa (PP2)	3/5 (60%) — deskriptif kuantitatif; sedang
Malik dkk. (2023) [46]	India; kurikulum AICTE	Studi kasus pemetaan kurikulum	Analisis dokumen (non-intervensi)	Kerangka pemetaan kurikulum ke KA CyBOK di konteks negara berkembang; masukan desain matriks kompetensi (PP2)	3/5 (60%) — kualitatif; sedang
Schafeitel-Tähtinen dkk. (2025) [47]	Finlandia & Ceko; sarjana	Kuasi-eksperimen pra-pasca; dua universitas	Laboratorium/CTF gamified	Efektivitas skenario CTF diukur pra-pasca lintas institusi; efek elemen gamifikasi bervariasi menurut kelompok mahasiswa (PP1, PP3)	4/5 (80%) — kuantitatif non-acak; tinggi
Guntoro dkk. (2026) [48]	Indonesia; SMK (vokasi)	Laporan pengabdian; 30 siswa	Rekonstruksi insiden nyata + diskusi	Pelatihan berbasis insiden dari berita lokal di SMKN 7 Pekanbaru; bukti langka konteks vokasi negara berkembang (PP4, PP5)	2/5 (40%) — deskriptif kuantitatif; rendah

PP1: Pendekatan dan Tipologi CBL

Penulis mengantisipasi kasus diskusi dan laboratorium paling sering dilaporkan, mencerminkan sifat ganda keamanan siber sebagai disiplin sosioteknis. Kasus terinterupsi, yang mensimulasikan pengungkapan informasi insiden secara progresif, diperkirakan menonjol dalam mata kuliah respons insiden. Kasus dilema dan jigsaw, yang menonjolkan dimensi etis dan multi-pemangku kepentingan, diantisipasi lebih jarang namun lebih banyak pada mata kuliah berorientasi tata kelola, risiko, dan kepatuhan (GRC). Antisipasi ini konsisten dengan temuan Ahmed dkk. [43] bahwa studi kasus, simulasi, dan laboratorium virtual mendominasi praktik pengajaran keamanan siber, serta dengan sintesis Matus dkk. [44] yang menunjukkan sentralitas lingkungan latihan serang-bertahan dalam literatur gamifikasi.

Temuan kunci yang diantisipasi adalah ketidaksesuaian antara keragaman tipologi dalam teori CBL [8,9,10] dan rentang tipe kasus yang lebih sempit dalam praktik keamanan siber. Tipe yang kurang dimanfaatkan, khususnya dilema dan jigsaw, mungkin sangat berharga untuk mengembangkan penalaran etis dan kompetensi komunikasi lintas fungsi yang secara konsisten diidentifikasi industri sebagai kurang berkembang pada lulusan [31].

PP2: Kompetensi yang Dikembangkan

Penulis membangun matriks kompetensi dua dimensi menggunakan area pengetahuan CyBOK [25] (baris) dan level Taksonomi Bloom yang direvisi [28] (kolom). Hipotesis: konsentrasi pada domain Serangan & Pertahanan dan Keamanan Sistem di level Menerapkan dan Menganalisis; domain Manusia, Organisasi & Regulasi yang mencakup konteks UU PDP [13] dan UU ITE [14], secara substansial kurang terwakili. Anderson dkk. [31] menemukan bahwa CBL untuk

 https://doi.org/10.56211/blendsains.v5i1.1833

pemimpin keamanan siber mengembangkan kemampuan metakognitif dan sikap professional, yaitu kompetensi yang sering diabaikan dalam pelatihan teknis murni. Ahmad dan Maynard [32] mendokumentasikan peningkatan kemampuan mahasiswa menalar tentang dimensi organisasi dan manusia dalam keamanan melalui kasus realistis. Sebagai model metodologis pemetaan, Kohnke, Tenbergen, dan Mead [45] mengembangkan pustaka 18 studi kasus yang dipetakan langsung ke area pengetahuan CyBOK dan mendokumentasikan peningkatan pemahaman mahasiswa; pendekatan pemetaan kurikulum ke CyBOK juga telah diterapkan Malik dkk. [46] pada kurikulum AICTE di India sebagai contoh konteks negara berkembang.

PP3: Pengukuran Efektivitas

Pengukuran efektivitas dalam penelitian CBL keamanan siber dicirikan oleh fragmentasi. Berdasarkan penjajakan awal, instrumen utama mencakup: (1) tes pengetahuan pra/pasca dengan keterbatasan validitas ekologis; (2) laporan kasus ber-rubrik untuk kualitas analitis; (3) survei perolehan belajar seperti instrumen Bonney [11] untuk persepsi kompetensi; (4) penilaian sejawat untuk kolaborasi; dan (5) penilaian berbasis kinerja dalam *cyber range* untuk keterampilan teknis. Desain pra-pasca lintas institusi seperti yang dilakukan Schafeitel-Tähtinen dkk. [47] pada skenario CTF di Finlandia dan Ceko menunjukkan arah pengukuran efektivitas yang lebih dapat dibandingkan antarpelajaran. Ahmad dan Maynard [32] memberikan bukti empiris bahwa kasus CBL realistis dalam manajemen keamanan informasi meningkatkan penalaran analitis dibandingkan format diskusi konvensional. Tidak adanya instrumen yang divalidasi secara psikometrik yang dirancang khusus untuk CBL keamanan siber tetap menjadi kesenjangan kritis, membatasi komparabilitas antarpelajaran.

PP4: Tantangan Implementasi

Tabel 3. Tantangan Implementasi CBL dalam Pendidikan Keamanan Siber

Kategori	Hambatan	Mitigasi
Etis & Hukum	Teknik ofensif tak dapat direplikasi pada sistem nyata; data pelanggaran nyata berisiko hukum di bawah UU PDP [13]	*Cyber range* terisolasi; data kasus difiktifkan; dokumen *Rules of Engagement* eksplisit
Infrastruktur	Biaya *cyber range* tinggi; *bandwidth lab cloud*; perangkat keras heterogen	Perangkat sumber terbuka (Kali Linux, OWASP WebGoat, Metasploitable); lab virtual berbasis *cloud*
Kemutakhiran Kasus	Lanskap ancaman berkembang cepat; kasus berbasis CVE spesifik usang dalam 12–24 bulan	Abstraksi ke level prinsip; protokol pembaruan kasus; ko-kreasi dengan industri
Kesiapan Instruktur	CBL membutuhkan keterampilan fasilitasi berbeda dari ceramah; penulisan kasus padat waktu	Catatan pengajaran per kasus; lokakarya; kalibrasi rubrik; model pengajaran tim
Kendala Institusional	Jam kredit kaku; kelas besar; sistem penilaian untuk pengujian objektif	Model kasus terbalik; desain modular; penilaian sejawat terintegrasi LMS

Sumber: Sintesis penulis berdasarkan literatur CBL dan keamanan siber

AGENDA PENELITIAN

Tabel 4. Matriks Agenda Penelitian CBL dalam Pendidikan Vokasi Keamanan Siber

No	Kesenjangan	Metodologi	Pertanyaan Penelitian Prioritas
1	Absennya studi empiris CBL di politeknik/vokasi	Kuasi-eksperimental; multi-situs; campuran	Apakah CBL berbeda efektivitasnya di konteks vokasi vs. universitas riset?
2	Tidak ada instrumen tervalidasi untuk kasus laboratorium CBL	Pengembangan skala (EFA/CFA); validasi pakar (CVR)	Properti psikometrik apa yang dimiliki rubrik untuk kasus laboratorium CBL keamanan siber?
3	Tidak ada studi retensi pengetahuan jangka panjang	Kohort longitudinal; post-test tertunda; kelompok kontrol	Apakah CBL menghasilkan retensi lebih baik pada 3, 6, dan 12 bulan vs. ceramah?

4	Belum ada kerangka CBL yang mengintegrasikan UU PDP dan UU ITE	Penelitian desain; validasi Delphi/CVR; kuasi-eksperimental	Bagaimana UU PDP [13] dan UU ITE [14] diintegrasikan ke dalam desain kasus CBL?
5	Efikasi diri dan identitas profesional melalui CBL belum diteliti	Survei longitudinal; SEM; fenomenologi kualitatif	Apakah CBL berkelanjutan menghasilkan perubahan terukur dalam efikasi diri keamanan siber [40]?
6	Keselarasan kasus CBL dengan industri belum dikaji empiris	Campuran; penilaian pemberi kerja; studi penelusur longitudinal	Apakah kasus CBL ko-kreasi industri menghasilkan kesiapan kerja lulusan lebih baik?

DISKUSI

Tema Kunci dan Implikasi

Tiga observasi antisipatif perlu dibahas. Pertama, dominasi kasus laboratorium berisiko mengabaikan dimensi sosioteknis pekerjaan keamanan. Anderson dkk. [31] menemukan bahwa CBL untuk pemimpin keamanan siber sangat efektif mengembangkan kemampuan metakognitif dan sikap professional, yaitu kompetensi yang kurang terlayani pendekatan berbasis laboratorium semata. Kurikulum CBL yang seimbang harus menangani dimensi teknis dan manusia keamanan siber, sebagaimana tercermin dalam luasnya CyBOK [25].

Kedua, fragmentasi instrumen pengukuran efektivitas merupakan hambatan signifikan bagi pembangunan pengetahuan kumulatif. Tanpa instrumen bersama yang tervalidasi, temuan studi individual tidak dapat dibandingkan secara bermakna. Pengembangan perangkat penilaian yang tervalidasi secara psikometrik untuk CBL keamanan siber akan memberikan kontribusi infrastruktur besar, analogis dengan instrumen perolehan belajar Bonney [11] untuk pendidikan biologi.

Ketiga, hampir tidak adanya konteks vokasi negara berkembang dalam literatur mewakili ketidakadilan struktural dalam produksi pengetahuan. Metode pengajaran atau riset di luar negeri tidak bisa langsung diterapkan di pendidikan vokasi di Indonesia, karena infrastruktur dan lingkungan belajarnya tidak sama. Literatur yang ada di konteks SMK Indonesia pun umumnya berformat pelatihan atau pengabdian masyarakat, misalnya pelatihan keamanan digital berbasis rekonstruksi insiden nyata di SMKN 7 Pekanbaru [48], bukan studi intervensi CBL yang dirancang dan diukur secara sistematis.

Implikasi untuk Modul CBL

Kerangka analitis ini memiliki implikasi desain langsung untuk modul CBL di Prodi RKS Politeknik Negeri Cilacap [16]: (1) diversifikasi tipe kasus dengan memasukkan kasus dilema (menonjolkan UU PDP dan UU ITE), jigsaw, dan terinterupsi selain kasus laboratorium; (2) integrasi regulasi, hukum pelindungan data dan kejahatan siber Indonesia harus tertanam dalam desain kasus; (3) desain pengukuran multiple, gabungan tes pengetahuan, rubrik laporan kasus, survei persepsi, dan penilaian sejawat; (4) catatan pengajaran per kasus termasuk panduan fasilitator, respons yang diantisipasi, dan contoh penilaian; (5) ko-kreasi industri dengan BSSN, ID-CERT, atau perusahaan keamanan siber swasta.

Keterbatasan

Keterbatasan TLS ini mencakup: (1) pembatasan bahasa Inggris dan Indonesia dapat memperkenalkan bias bahasa; (2) inklusi prosiding konferensi memperkenalkan risiko temuan tidak lengkap, dimitigasi penilaian kualitas; (3) lanskap ancaman yang berkembang cepat berarti beberapa desain kasus dalam studi yang diinklusikan mungkin sudah usang; (4) sebagai naskah pra-registrasi, dokumen ini menyajikan temuan yang diantisipasi, bukan aktual.

KESIMPULAN DAN SARAN

TLS ini mengisi kesenjangan signifikan dalam penelitian pendidikan keamanan siber: tidak adanya sintesis komprehensif dan metodologis ketat tentang pendekatan CBL, luaran, dan tantangan dalam disiplin ini. Menggunakan protokol PRISMA 2020, kerangka lima-PP yang terstruktur, dan penilaian kualitas melalui MMAT yang diadaptasi, tinjauan ini akan menghasilkan: (1) peta sistematis pertama tipologi CBL dalam pendidikan keamanan siber; (2) analisis cakupan kompetensi yang diselaraskan dengan CyBOK dan NIST CSF 2.0; (3) katalog instrumen pengukuran efektivitas; (4)

analisis terstruktur tantangan implementasi dengan perhatian khusus pada kendala etis-hukum; dan (5) agenda penelitian enam-tema untuk CBL dalam pendidikan vokasi keamanan siber di negara berkembang.

Bagi Prodi RKS Politeknik Negeri Cilacap, tinjauan ini menyediakan basis bukti sekaligus kerangka desain modul CBL. Agenda penelitian mendefinisikan program studi empiris yang dapat dilaksanakan dalam prodi untuk berkontribusi pada basis pengetahuan global sambil meningkatkan praktik pendidikan lokal. Lebih luas lagi, TLS ini memajukan argumen bahwa penelitian pendidikan keamanan siber harus lebih beragam secara global: kesenjangan keterampilan paling akut terjadi justru pada latar institusional—politeknik vokasi di negara berkembang—yang paling kurang terwakili dalam literatur. Menutup kesenjangan pengetahuan tersebut adalah prasyarat untuk menutup kesenjangan bakat.

Saran

Berdasarkan pemetaan konseptual dan agenda penelitian di atas, beberapa saran diajukan bagi pihak terkait. Bagi Program Studi Rekayasa Keamanan Siber Politeknik Negeri Cilacap, disarankan untuk: (1) mendiversifikasi tipe kasus dengan tidak hanya bertumpu pada kasus laboratorium, tetapi juga memasukkan kasus dilema, jigsaw, dan terinterupsi yang menonjolkan dimensi etis, hukum, dan lintas-fungsi; (2) menanamkan kerangka regulasi nasional, khususnya UU Pelindungan Data Pribadi No. 27/2022 dan UU ITE No. 11/2008, secara eksplisit ke dalam desain kasus; (3) memanfaatkan cyber range berbasis perangkat sumber terbuka untuk menekan biaya infrastruktur; (4) menyusun catatan pengajaran per kasus serta menyelenggarakan lokakarya fasilitasi dan kalibrasi rubrik bagi dosen; dan (5) menjalin ko-kreasi kasus dengan BSSN, ID-CERT, atau industri agar kasus relevan dengan kebutuhan kerja.

Bagi peneliti selanjutnya, disarankan untuk: (1) melaksanakan studi kuasi-eksperimental multi-situs yang membandingkan efektivitas CBL pada konteks pendidikan vokasi dan universitas riset; (2) mengembangkan serta memvalidasi instrumen penilaian yang teruji secara psikometrik khusus untuk CBL keamanan siber guna mengatasi fragmentasi pengukuran; (3) melakukan studi retensi longitudinal untuk menilai daya tahan pembelajaran; dan (4) membangun kerangka integrasi regulasi ke dalam desain kasus melalui penelitian desain dan validasi pakar.

Bagi institusi dan pemangku kebijakan, disarankan untuk mendorong keterwakilan konteks pendidikan vokasi di negara berkembang dalam publikasi ilmiah, serta menyediakan dukungan pendanaan dan infrastruktur laboratorium yang memadai sebagai prasyarat penerapan CBL yang berkelanjutan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada tim Program Studi Rekayasa Keamanan Siber Politeknik Negeri Cilacap atas diskusi dan dukungan yang berharga dalam pengembangan panduan CBL yang menjadi motivasi penelitian ini [16].

DAFTAR PUSTAKA

[1] ISC2, "Cybersecurity Workforce Study 2023," ISC2, 2023. [Daring]. Tersedia: https://www.isc2.org/research/workforce-study
[2] Badan Siber dan Sandi Negara (BSSN), Laporan Tahunan Keamanan Siber Indonesia 2023. Jakarta: BSSN, 2024.
[3] Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99.
[4] K. Nance, B. Hay, dan M. Bishop, "Investigating the endemic culture of cybersecurity and how education can be used as a catalyst for change," dalam Pros. HICSS ke-42, IEEE, 2009, hlm. 1–7, doi: 10.1109/HICSS.2009.176.
[5] B. Krebs, R. Arora, S. Masciola, N. C. Rowe, dan T. Johnsen, "Addressing the cybersecurity education gap: An integrative review of teaching approaches," Educ. Inf. Technol., vol. 27, no. 5, hlm. 6843–6875, 2022, doi: 10.1007/s10639-021-10830-z.
[6] L. S. Vygotsky, Mind in Society: The Development of Higher Psychological Processes. Cambridge, MA: Harvard University Press, 1978.
[7] J. Lave dan E. Wenger, Situated Learning: Legitimate Peripheral Participation. Cambridge: Cambridge University Press, 1991, doi: 10.1017/CBO9780511815355.
[8] C. F. Herreid, "Case studies in science—a novel method of science education," J. Coll. Sci. Teach., vol. 23, no. 4, hlm. 221–229, 1994.
[9] C. F. Herreid, "The interrupted case method," J. Coll. Sci. Teach., vol. 35, no. 2, hlm. 4–5, 2005.

[10] C. F. Herreid, "Case study teaching," New Dir. Teach. Learn., vol. 2011, no. 128, hlm. 31–40, 2011, doi: 10.1002/tl.466.
[11] K. M. Bonney, "Case study teaching method improves student performance and perceptions of learning gains," J. Microbiol. Biol. Educ., vol. 16, no. 1, hlm. 21–28, 2015, doi: 10.1128/jmbe.v16i1.846.
[12] V. Kulak dan G. Newton, "A guide to using case-based learning in biochemistry education," Biochem. Mol. Biol. Educ., vol. 42, no. 6, hlm. 457–473, 2014, doi: 10.1002/bmb.20823.
[13] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
[14] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.
[15] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, dkk., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, n71, 2021, doi: 10.1136/bmj.n71.
[16] Politeknik Negeri Cilacap, Panduan Pembelajaran Berbasis Kasus (CBL): Rekayasa Keamanan Siber (RKS-PNC). Cilacap: Politeknik Negeri Cilacap, 2025.
[17] B. Schneier, Secrets and Lies: Digital Security in a Networked World, Ed. ke-15. Hoboken, NJ: Wiley, 2015.
[18] M. E. Whitman dan H. J. Mattord, Management of Information Security, Ed. ke-6. Boston: Cengage Learning, 2021.
[19] M. Bishop, Computer Security: Art and Science, Ed. ke-2. Upper Saddle River, NJ: Pearson, 2019.
[20] D. A. Kolb, Experiential Learning: Experience as the Source of Learning and Development, Ed. ke-2. Upper Saddle River, NJ: FT Press / Pearson Education, 2014.
[21] M. S. Knowles, E. F. Holton, dan R. A. Swanson, The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development, Ed. ke-9. New York: Routledge, 2020.
[22] J. R. Savery, "Overview of problem-based learning: Definitions and distinctions," Interdiscip. J. Probl.-Based Learn., vol. 1, no. 1, hlm. 9–20, 2006, doi: 10.7771/1541-5015.1002.
[23] M. J. Newman, "Problem based learning: An introduction and overview of the key features of the approach," J. Vet. Med. Educ., vol. 32, no. 1, hlm. 12–20, 2005, doi: 10.3138/jvme.32.1.12.
[24] D. H. Jonassen dan W. Hung, "All problems are not equal: Implications for problem-based learning," Interdiscip. J. Probl.-Based Learn., vol. 2, no. 2, hlm. 6–28, 2008, doi: 10.7771/1541-5015.1080.
[25] A. Rashid, H. Chivers, G. Danezis, E. Lupu, dan A. Martin, Eds., The Cyber Security Body of Knowledge (CyBOK) v1.1. Bristol: Universitas Bristol / National Cyber Security Centre, 2021. [Daring]. Tersedia: https://www.cybok.org
[26] National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST, 2024, CSWP 29, doi: 10.6028/NIST.CSWP.29.
[27] B. S. Bloom, M. D. Engelhart, E. J. Furst, W. H. Hill, dan D. R. Krathwohl, Taxonomy of Educational Objectives: Handbook I – Cognitive Domain. New York: David McKay Company, 1956.
[28] L. W. Anderson dan D. R. Krathwohl, Eds., A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. New York: Longman, 2001.
[29] B. Krebs dkk., "Addressing the cybersecurity education gap," Educ. Inf. Technol., vol. 27, no. 5, hlm. 6843–6875, 2022, doi: 10.1007/s10639-021-10830-z. [Sama dengan [5]; dipertahankan untuk konsistensi urutan sitasi]
[30] L. Tobarra, A. Robles-Gomez, S. Ros, R. Hernandez, dan A. C. Caminero, "A survey of game-based learning in cybersecurity education," Comput. Secur., vol. 128, 103146, 2023, doi: 10.1016/j.cose.2023.103146.
[31] A. Anderson, A. Ahmad, dan S. Chang, "Case-based learning for cybersecurity leaders: A systematic review and research agenda," Inf. Manag., vol. 61, no. 7, 104015, 2024, doi: 10.1016/j.im.2024.104015.
[32] A. Ahmad dan S. B. Maynard, "Teaching information security management: Reflections on effective and ineffective pedagogical approaches," Inf. Manag. Comput. Secur., vol. 22, no. 5, hlm. 427–442, 2014, doi: 10.1108/IMCS-07-2013-0052.
[33] D. Tranfield, D. Denyer, dan P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," Br. J. Manag., vol. 14, no. 3, hlm. 207–222, 2003, doi: 10.1111/1467-8551.00375.
[34] Q. N. Hong, P. Pluye, S. Fabregues, G. Bartlett, F. Boardman, M. Cargo, dkk., Mixed Methods Appraisal Tool (MMAT) Version 2018. Montreal: Universitas McGill, 2018.
[35] J. Popay, H. Roberts, A. Sowden, M. Petticrew, L. Arai, M. Rodgers, dkk., Guidance on the Conduct of Narrative Synthesis in Systematic Reviews. Lancaster: Lancaster University (ESRC Methods Programme), 2006.
[36] D. Thomas, "A general inductive approach for analyzing qualitative evaluation data," Am. J. Eval., vol. 27, no. 2, hlm. 237–246, 2006, doi: 10.1177/1098214005283748.
[37] Mahardika, F., … E. S.-S. J. T., & 2019, undefined. (n.d.). Penerapan Segmentasi Warna pada Gambar di Media Sosial dengan Algoritma Fuzzy K-Means Cluster. *Ojs3-Jurnal.Umk.Ac.Id*. Retrieved December 19, 2025, from

https://ojs3-jurnal.umk.ac.id/index.php/simet/article/view/3381

[38] Mahardika, F., … L. S.-J. T. I., & 2026, undefined. (2026). IoT-Based Smart Detector with SVM and XGBoost for Real-Time Child Growth Monitoring and Stunting Risk Prediction. *Jutif.If.Unsoed.Ac.IdF Mahardika, L Syafirullah, A NugrohoJurnal Teknik Informatika (Jutif), 2026•jutif.If.Unsoed.Ac.Id*, *7*(1), 2723–3863. https://doi.org/10.52436/1.jutif.2026.7.2.5394

[39] Mahardika, F., Setiawan, E., Intan, D., & Saputra, S. (2019). PENERAPAN SEGMENTASI WARNA PADA GAMBAR DI MEDIA SOSIAL DENGAN ALGORITMA FUZZY K-MEANS CLUSTER. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *10*(2), 631–638. https://doi.org/10.24176/SIMET.V10I2.338

[40] A. Bandura, Self-Efficacy: The Exercise of Control. New York: Freeman, 1997.

[41] Y. Cai, "Using case studies to teach cybersecurity courses," J. Cybersecur. Educ. Res. Pract., vol. 2018, no. 2, Artikel 1, 2018.

[42] Syafirullah, L., Mahardika, F., Purwanto, R., Prasetyanti, D. N., Rekayasa, T., Lunak, P., Cilacap, P. N., Informatika, T., & Cilacap, P. N. (2026). *Performance Evaluation and Optimization of an IoT-Based Fish Smoking Monitoring System for Ensuring Product Quality*. *10*(1), 691–700.

[43] A. Ahmed, C. Watterson, S. Alhashmi, dan T. Gaber, "How universities teach cybersecurity courses online: a systematic literature review," Front. Comput. Sci., vol. 6, 1499490, 2024, doi: 10.3389/fcomp.2024.1499490.

[44] N. Matus, S. Berríos, dan R. Isla, "From CTF to competence: UX-driven and didactic foundations for gamified cybersecurity training platforms," Appl. Sci., vol. 16, no. 12, 6100, 2026, doi: 10.3390/app16126100.

[45] A. Kohnke, B. Tenbergen, dan N. Mead, "Using Cybersecurity Body of Knowledge (CyBOK) case studies to enhance student learning," dalam Pros. Hawaii Int. Conf. Syst. Sci. (HICSS) ke-55, 2022, hlm. 1–10, doi: 10.24251/HICSS.2022.130.

[46] P. Malik, A. Kumar Singh, R. Nautiyal, dan S. Rawat, "Mapping AICTE cybersecurity curriculum onto CyBOK: a case study," dalam Machine Learning for Cyber Security, Berlin: De Gruyter, 2023, hlm. 129–144, doi: 10.1515/9783110766745-007.

[47] T. Schafeitel-Tähtinen dkk., "Teaching and learning cybersecurity using capture the flag: Effectiveness comparison between university students in Finland and Czechia," Comput. Appl. Eng. Educ., vol. 33, e70082, 2025, doi: 10.1002/cae.70082.

[48] G. Guntoro, L. Lisnawita, W. Monika, dan L. Costaner, "Empowering vocational school students through digital security training to prevent cyber threats: A case study at SMKN 7 Pekanbaru," CONSEN: Indones. J. Community Serv. Engagem., vol. 6, no. 1, hlm. 48–54, 2026, doi: 10.57152/consen.v6i1.2326.