

Pelatihan Literasi Digital dan Keamanan Siber bagi Anggota CSIRT di Kabupaten Madiun

Digital Literacy and Cybersecurity Training for CSIRT Members in Madiun Regency

Andria^{*1}, Mei Lenawati², Pika Dinelia³

^{1,2,3} Program Studi Sistem Informasi, Fakultas Teknik, Universitas PGRI Madiun

e-mail: ^{1*}andria@unipma.ac.id, ²mei.lenawati@unipma.ac.id,

³pika_2405102003@mhs.unipma.ac.id

Abstrak - Peningkatan kapasitas sumber daya manusia di bidang literasi digital dan keamanan siber merupakan kebutuhan mendesak bagi aparat pemerintah daerah dalam menghadapi transformasi digital yang semakin masif. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan kompetensi anggota Computer Security Incident Response Team (CSIRT) di Kabupaten Madiun melalui pelatihan terstruktur yang mencakup empat pilar literasi digital: Digital Skills, Digital Safety, Digital Ethics, dan Digital Culture, serta keterampilan teknis keamanan siber. Metode pelaksanaan menggunakan pendekatan partisipatif dengan kombinasi ceramah interaktif, demonstrasi langsung, praktik hands-on, studi kasus insiden nyata, dan evaluasi berbasis pre-test dan post-test. Kegiatan dilaksanakan selama periode November 2025 hingga Juli 2026 di Dinas Komunikasi dan Informatika Kabupaten Madiun dengan 30 peserta dari berbagai OPD. Hasil kegiatan menunjukkan peningkatan rata-rata skor literasi digital sebesar 62,3% dan pemahaman keamanan siber sebesar 70,8%. Seluruh peserta menyatakan materi relevan dengan tugas operasional CSIRT, dan 93,3% merekomendasikan program ini dilanjutkan secara berkala. Kegiatan pengabdian ini memberikan kontribusi nyata dalam membangun budaya keamanan siber yang berkelanjutan di lingkungan pemerintah daerah Kabupaten Madiun.

Kata kunci – CSIRT ; keamanan siber ; literasi digital ; pengabdian masyarakat ; pemerintah daerah

Abstract - Increasing the capacity of human resources in digital literacy and cybersecurity was an urgent need for local government officials amid rapid digital transformation. This community service activity aimed to enhance the competencies of Computer Security Incident Response Team (CSIRT) members in Madiun Regency through structured training covering four digital literacy pillars: Digital Skills, Digital Safety, Digital Ethics, and Digital Culture, alongside technical cybersecurity skills. The implementation method used a participatory approach combining interactive lectures, live demonstrations, hands-on practice, real incident case studies, and pre-test/post-test evaluation. The activity was conducted from November 2025 to July 2026 at the Communication and Information Technology Office of Madiun Regency, involving 30 participants from various regional government units. Results showed an average increase of 62.3% in digital literacy scores and 70.8% in cybersecurity understanding. All participants stated the material was relevant to CSIRT operational duties, and 93.3% recommended the program be continued on a regular basis. This community service activity made a tangible contribution to building a sustainable cybersecurity culture in Madiun Regency's local government environment.

Keywords – community service ; CSIRT ; cybersecurity ; digital literacy ; local government

I. PENDAHULUAN

Transformasi digital yang berlangsung pesat di sektor pemerintahan Indonesia membawa konsekuensi ganda: di satu sisi meningkatkan efisiensi dan kualitas layanan publik, namun di sisi lain memperluas permukaan serangan (attack surface) terhadap infrastruktur sistem informasi pemerintah. Berdasarkan Lanskap Keamanan Siber Indonesia 2024 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), sektor pemerintahan daerah menjadi salah satu target utama ancaman siber, termasuk serangan ransomware, phishing, dan kebocoran data pribadi [1]. Kondisi ini menuntut setiap aparat pemerintah, terutama yang tergabung dalam tim keamanan siber, untuk memiliki literasi digital dan kecakapan teknis keamanan siber yang memadai.

Kabupaten Madiun merupakan salah satu dari delapan kabupaten/kota di Jawa Timur yang telah membentuk Computer Security Incident Response Team (CSIRT), dikenal sebagai MadiunKab-CSIRT, yang beroperasi di bawah Dinas Komunikasi dan Informatika (Diskominfo). Tim ini bertugas memberikan peringatan keamanan informasi, mengkoordinasikan penanganan insiden siber, serta memberikan edukasi kepada OPD di lingkungan pemerintah daerah [2]. Meskipun struktur organisasi CSIRT telah terbentuk, kapasitas anggota dalam hal literasi digital dan kompetensi teknis keamanan siber masih memerlukan peningkatan yang terstruktur dan berkelanjutan.

Literasi digital didefinisikan sebagai kemampuan individu dalam mengenali, memahami, mengevaluasi, dan memanfaatkan informasi melalui media digital dan jejaring internet [3]. Kementerian Komunikasi dan Informatika (Kominfo) merumuskan kerangka literasi digital dalam Roadmap Literasi Digital 2021-2024 yang mencakup empat pilar: Digital Skills, Digital Safety, Digital Ethics, dan Digital Culture. Hasil Indeks Literasi Digital Indonesia 2021 menunjukkan bahwa pilar Digital Safety memperoleh skor terendah (3,10 dari skala 5), mengindikasikan bahwa kemampuan masyarakat—termasuk aparat pemerintah—dalam melindungi diri di ruang siber masih perlu ditingkatkan secara signifikan [4].

Program pelatihan literasi digital untuk Aparatur Sipil Negara (ASN) sektor pemerintahan telah diinisiasi secara nasional oleh Kominfo melalui program ASN Makin Cakap Digital, yang pada tahun 2024 berhasil menjangkau lebih dari 80.000 ASN di berbagai kementerian/lembaga [5]. Namun, program nasional tersebut bersifat umum dan belum secara spesifik mengakomodasi kebutuhan teknis anggota CSIRT yang memerlukan kompetensi keamanan siber lebih mendalam. Kegiatan pengabdian kepada masyarakat ini dirancang untuk mengisi kesenjangan tersebut dengan menyusun kurikulum pelatihan yang mengintegrasikan empat pilar literasi digital dengan keterampilan teknis keamanan siber yang relevan dengan tugas operasional CSIRT.

Penelitian terdahulu mengenai pelatihan keamanan siber bagi pegawai pemerintah menunjukkan bahwa pendekatan partisipatif dan berbasis kasus nyata secara signifikan meningkatkan kesadaran dan perubahan perilaku keamanan dibandingkan pelatihan konvensional yang bersifat satu arah [6], [7]. Kebaruan kegiatan pengabdian ini terletak pada integrasi kurikulum empat pilar literasi digital Kominfo dengan modul keamanan siber operasional CSIRT dalam satu program pelatihan terpadu yang disesuaikan dengan konteks pemerintahan daerah di Kabupaten Madiun. Tujuan kegiatan ini adalah meningkatkan kompetensi literasi digital dan keamanan siber anggota CSIRT Kabupaten Madiun sehingga mampu menjalankan fungsi edukasi, pencegahan, dan penanganan insiden siber secara lebih efektif.

II. METODE

A. Desain Kegiatan

Kegiatan pengabdian kepada masyarakat ini dirancang menggunakan pendekatan Action Research yang bersifat siklus, terdiri dari empat tahapan: (1) Identifikasi Kebutuhan (Needs Assessment), (2) Perancangan dan Persiapan Program, (3) Pelaksanaan Pelatihan, dan (4) Evaluasi dan Tindak Lanjut. Kegiatan dilaksanakan pada periode 04 November 2025 hingga 31 Juli 2026 di Dinas Komunikasi dan Informatika Kabupaten Madiun, dengan total 20 sesi pelatihan yang terdistribusi secara bertahap selama delapan bulan.

B. Peserta Kegiatan

Sasaran kegiatan adalah 30 orang anggota MadiunKab-CSIRT yang terdiri dari pegawai Diskominfo Kabupaten Madiun dan perwakilan OPD tingkat kecamatan. Penetapan peserta dilakukan secara purposive berdasarkan rekomendasi Kepala Diskominfo Kabupaten Madiun, dengan mempertimbangkan relevansi tugas dan fungsi peserta terhadap pengelolaan keamanan informasi di masing-masing satuan kerja.

C. Materi dan Kurikulum Pelatihan

Kurikulum pelatihan disusun berdasarkan hasil analisis kebutuhan awal yang melibatkan diskusi kelompok terfokus (FGD) dengan perwakilan anggota CSIRT dan pengamatan langsung kondisi kapabilitas teknis. Materi pelatihan mencakup dua komponen utama: (1) Literasi Digital berbasis empat pilar Kominfo, dan (2) Keamanan Siber Operasional CSIRT. Tabel 1 menyajikan struktur kurikulum lengkap program pelatihan.

Tabel 1. Kurikulum Pelatihan Literasi Digital dan Keamanan Siber

Sesi	Materi	Pilar / Komponen	Metode	Durasi
1-2	Pengantar Literasi Digital & Transformasi Digital Pemerintahan	Digital Culture	Ceramah, Diskusi	4 jam
3-4	Etika Bermedia Digital & Pengelolaan Informasi Publik	Digital Ethics	Studi Kasus, Diskusi	4 jam
5-6	Kecakapan Digital: Aplikasi Produktivitas & Kolaborasi Online	Digital Skills	Hands-on Practice	4 jam
7-8	Perlindungan Data Pribadi & Privasi Digital	Digital Safety	Ceramah, Simulasi	4 jam
9-10	Pengantar Keamanan Siber & Lanskap Ancaman	Keamanan Siber	Ceramah, Video Kasus	4 jam
11-12	Pengenalan & Mitigasi Social Engineering (Phishing, Vishing)	Digital Safety + Siber	Simulasi Phishing	4 jam
13-14	Manajemen Insiden Siber & Prosedur CSIRT	Keamanan Siber	Studi Kasus, Roleplay	4 jam
15-16	Keamanan Jaringan & Monitoring Lalu Lintas Data	Keamanan Siber	Praktik Wireshark	4 jam

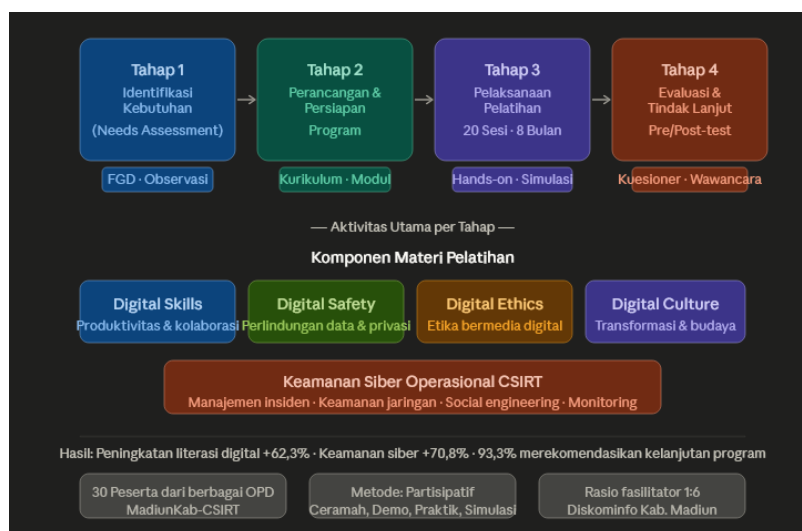
Sesi	Materi	Pilar / Komponen	Metode	Durasi
17- 18	Keamanan Sistem Informasi Pemerintah & SPBE	Digital Safety + Siber	Diskusi, Simulasi	4 jam
19- 20	Evaluasi Komprehensif, Post-test & Rencana Tindak Lanjut	Semua Pilar	Post-test, Presentasi	4 jam

D. Metode Pelaksanaan

Pelaksanaan pelatihan menggunakan pendekatan partisipatif dengan variasi metode pembelajaran untuk memaksimalkan keterlibatan dan retensi pengetahuan peserta. Metode yang digunakan meliputi: (1) ceramah interaktif dengan tanya jawab; (2) demonstrasi langsung tools digital dan keamanan siber; (3) praktik hands-on dengan pendampingan fasilitator; (4) studi kasus insiden keamanan siber nyata yang pernah terjadi pada instansi pemerintah Indonesia; (5) simulasi skenario insiden dan roleplay penanganan; serta (6) diskusi kelompok dan berbagi pengalaman antar peserta. Rasio fasilitator terhadap peserta dijaga pada 1:6 untuk memastikan kualitas pendampingan praktik.

E. Instrumen Evaluasi

Evaluasi dilakukan pada tiga tingkatan: (1) evaluasi reaksi peserta menggunakan kuesioner kepuasan di setiap akhir sesi; (2) evaluasi pembelajaran melalui pre-test sebelum pelatihan dimulai dan post-test di akhir program, masing-masing terdiri dari 50 butir soal yang mencakup seluruh komponen materi; dan (3) evaluasi penerapan melalui observasi dan wawancara tindak lanjut tiga bulan setelah pelatihan berakhir. Data dianalisis menggunakan statistik deskriptif dan uji perbandingan skor pre-test dan post-test.



Gambar 1. Tahapan Pelaksanaan Program Pengabdian Masyarakat

III. HASIL DAN PEMBAHASAN

A. Profil Peserta dan Kondisi Awal

Dari 30 peserta yang mengikuti kegiatan pelatihan, 60% (18 orang) berjenis kelamin laki-laki dan 40% (12 orang) perempuan. Berdasarkan latar belakang pendidikan, 50% memiliki jenjang Sarjana bidang TIK, 30% Sarjana non-TIK, dan 20% Diploma III. Berdasarkan masa

kerja, 40% telah bekerja lebih dari 10 tahun, 35% antara 5-10 tahun, dan 25% kurang dari 5 tahun. Hasil pre-test menunjukkan rata-rata skor literasi digital sebesar 46,2 dari skala 100, sedangkan pemahaman keamanan siber rata-rata 41,5. Skor Digital Safety merupakan yang terendah di antara empat pilar literasi digital (40,8), selaras dengan temuan Indeks Literasi Digital Nasional yang menunjukkan pilar keamanan digital sebagai titik lemah terbesar.

Tabel 2. Profil Peserta Pelatihan Berdasarkan Latar Belakang

Kategori	Sub-Kategori	Jumlah	Persentase
Jenis Kelamin	Laki-laki	18 orang	60%
	Perempuan	12 orang	40%
Pendidikan	S1 Bidang TIK	15 orang	50%
	S1 Non-TIK	9 orang	30%
	Diploma III	6 orang	20%
Masa Kerja	> 10 Tahun	12 orang	40%
	5 – 10 Tahun	10 orang	33,3%
	< 5 Tahun	8 orang	26,7%

B. Hasil Evaluasi Pre-Test dan Post-Test

Setelah mengikuti 20 sesi pelatihan selama delapan bulan, seluruh peserta menunjukkan peningkatan skor yang signifikan pada seluruh dimensi. Tabel 3 menyajikan perbandingan rata-rata skor pre-test dan post-test per pilar literasi digital dan komponen keamanan siber.

Tabel 3. Hasil Pre-Test dan Post-Test per Dimensi Kompetensi

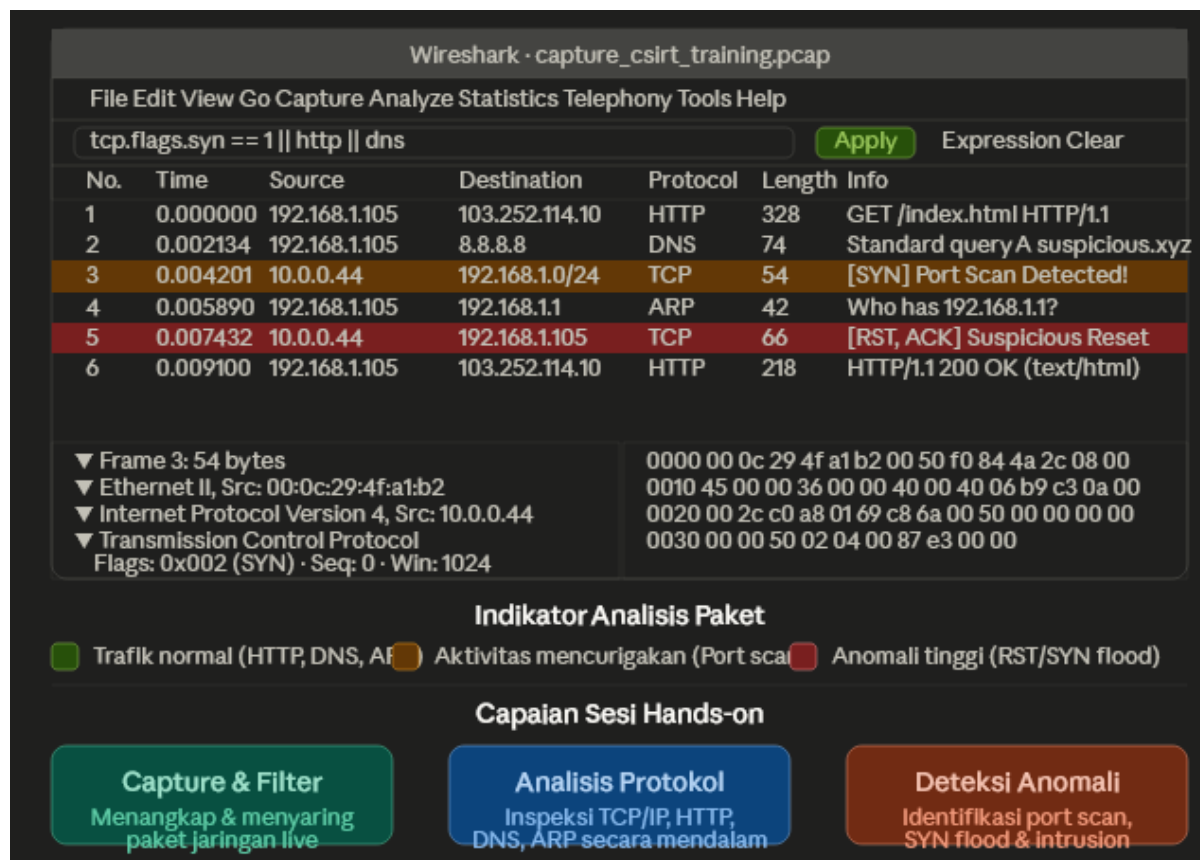
No	Dimensi	Rata-rata Pre-test	Rata-rata Post-test	Peningkatan (%)
1	Digital Skills	48,4	76,2	57,4%
2	Digital Safety	40,8	72,4	77,5%
3	Digital Ethics	52,6	80,0	52,1%
4	Digital Culture	43,8	74,6	70,3%
5	Keamanan Siber Dasar	42,0	71,8	71,0%
6	Manajemen Insiden CSIRT	40,6	70,2	73,0%
7	Keamanan Jaringan Pemerintahan	41,8	69,6	66,5%
	Rata-rata Keseluruhan	44,3	73,5	66,0%

Peningkatan tertinggi terjadi pada dimensi Digital Safety (77,5%), yang mengindikasikan efektivitas modul perlindungan data pribadi, simulasi phishing, dan praktik keamanan akun digital. Hal ini selaras dengan temuan penelitian bahwa pelatihan berbasis simulasi skenario nyata secara signifikan lebih efektif dalam membangun kesadaran keamanan digital dibandingkan pendekatan berbasis teks saja [8]. Peningkatan pada dimensi Digital Ethics (52,1%) merupakan yang paling moderat, karena sebagian peserta dengan pengalaman kerja panjang telah memiliki pemahaman dasar etika digital dalam konteks layanan publik.

C. Capaian per Sesi dan Dinamika Pembelajaran

Evaluasi per sesi menunjukkan tingkat kehadiran rata-rata 96,3% sepanjang program. Sesi dengan keterlibatan peserta tertinggi adalah sesi simulasi phishing (Sesi 11-12), di mana seluruh peserta berhasil mengidentifikasi minimal 8 dari 10 sampel email phishing setelah

mendapat pembekalan materi. Sesi studi kasus insiden nyata (Sesi 13-14) memperoleh skor kepuasan tertinggi (rata-rata 4,7 dari skala 5) karena peserta dapat menghubungkan materi langsung dengan potensi insiden yang mungkin terjadi di OPD masing-masing.



Gambar 2. Sesi Pelatihan Hands-on Keamanan Jaringan dengan Wireshark

D. Hasil Evaluasi Kepuasan dan Dampak Pelatihan

Kuesioner evaluasi kepuasan yang disebar di akhir program diisi oleh seluruh 30 peserta. Tabel 4 merangkum hasil evaluasi kepuasan peserta terhadap berbagai aspek program pelatihan.

Tabel 4. Hasil Evaluasi Kepuasan Peserta Program Pelatihan

Aspek Evaluasi	Sangat Puas / Setuju	Puas / Setuju	Kurang
Relevansi materi dengan tugas CSIRT	70,0%	30,0%	0%
Kualitas penyampaian materi oleh fasilitator	66,7%	30,0%	3,3%
Metode pelatihan hands-on dan simulasi	76,7%	20,0%	3,3%
Manfaat praktis materi Digital Safety	73,3%	26,7%	0%
Studi kasus insiden nyata pemerintah Indonesia	80,0%	16,7%	3,3%
Dukungan fasilitas dan infrastruktur pelatihan	56,7%	36,7%	6,6%

Aspek Evaluasi	Sangat Puas / Setuju	Puas / Setuju	Kurang
Program perlu dilanjutkan secara berkala	83,3%	10,0%	6,7%

Secara keseluruhan, 93,3% peserta menyatakan program pelatihan perlu dilanjutkan secara berkala. Aspek yang paling banyak mendapat respons sangat puas adalah penggunaan studi kasus insiden nyata (80,0%) dan metode hands-on serta simulasi (76,7%). Satu-satunya aspek yang mendapat catatan kekurangan adalah fasilitas dan infrastruktur, terkait kapasitas laboratorium komputer yang belum sepenuhnya memadai untuk 30 peserta bersamaan dalam sesi praktik jaringan.

E. Pembahasan dan Implikasi

Hasil kegiatan pengabdian ini menunjukkan efektivitas yang signifikan dalam meningkatkan kompetensi literasi digital dan keamanan siber anggota CSIRT Kabupaten Madiun. Peningkatan rata-rata skor sebesar 66,0% mengkonfirmasi bahwa pendekatan pelatihan partisipatif yang mengintegrasikan materi literasi digital empat pilar Kominfo dengan keterampilan teknis keamanan siber memberikan dampak nyata bagi peserta dari berbagai latar belakang [3], [6]. Temuan ini konsisten dengan penelitian Abrahams et al. (2024) yang menyimpulkan bahwa program edukasi keamanan siber yang menggabungkan simulasi skenario nyata, umpan balik berkala, dan pembelajaran berbasis kasus menghasilkan peningkatan kesadaran dan perubahan perilaku yang lebih sustain dibandingkan pelatihan berbasis modul statis [9].

Dari perspektif pengabdian kepada masyarakat, program ini memiliki dampak ganda: pertama, peningkatan kapabilitas teknis anggota CSIRT secara langsung; kedua, meningkatnya kemampuan anggota CSIRT dalam menyebarluaskan pengetahuan keamanan siber kepada rekan kerja di OPD masing-masing (multiplier effect). Hasil wawancara tindak lanjut tiga bulan setelah pelatihan menunjukkan bahwa 20 dari 30 peserta (66,7%) telah menginisiasi sosialisasi keamanan siber minimal satu kali di OPD-nya masing-masing, mengindikasikan terjadinya transfer pengetahuan yang berkelanjutan.



Gambar 3. Peserta Berdiskusi dalam Sesi Studi Kasus Insiden Siber Nyata

IV. KESIMPULAN DAN SARAN

Kegiatan pengabdian kepada masyarakat berupa pelatihan literasi digital dan keamanan siber bagi anggota CSIRT Kabupaten Madiun yang dilaksanakan selama periode November 2025 hingga Juli 2026 di Dinas Komunikasi dan Informatika Kabupaten Madiun telah berhasil meningkatkan kompetensi peserta secara signifikan, ditunjukkan oleh peningkatan rata-rata skor evaluasi sebesar 66,0% dengan peningkatan tertinggi pada pilar Digital Safety (77,5%) dan Manajemen Insiden CSIRT (73,0%), serta tingkat kepuasan peserta yang tinggi dengan 93,3% merekomendasikan keberlanjutan program. Kegiatan ini merekomendasikan: (1) keberlanjutan program pelatihan secara berkala minimal dua kali per tahun dengan penambahan modul ancaman siber terkini; (2) peningkatan kapasitas laboratorium komputer Diskominfo Kabupaten Madiun untuk mendukung praktik jaringan skala lebih besar; (3) pengembangan modul lanjutan yang mencakup topik keamanan cloud, forensik digital, dan respons insiden terhadap serangan Advanced Persistent Threat (APT); serta (4) penerapan model pelatihan terpadu ini sebagai rujukan bagi CSIRT pemerintah daerah lain di Jawa Timur dan nasional.

DAFTAR PUSTAKA

- [1] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2024," BSSN, Jakarta, pp. 1-107, 2025.
- [2] MadiunKab-CSIRT, "Profil MadiunKab-CSIRT," Dinas Komunikasi dan Informatika Kabupaten Madiun, 2024. [Online]. Available: <https://csirt.madiunkab.go.id/portal/profil>
- [3] Kementerian Komunikasi dan Informatika RI, "Roadmap Literasi Digital Indonesia 2021-2024," Kominfo, Jakarta, 2021.

- [4] Katadata Insight Center dan Kominfo RI, "Status Literasi Digital Indonesia 2021: Hasil Survei di 34 Provinsi," Kominfo, Jakarta, 2021.
- [5] Kementerian Komunikasi dan Informatika RI, "80.000 ASN Kemendikbudristek Perkuat Literasi Digital melalui Program LDSP," Siaran Pers No. 49/HM/KOMINFO/04/2023, Apr. 2024. [Online]. Available: <https://www.kemdikbud.go.id/main/blog/2024/03>
- [6] T. S. Chew, "Considerations for Developing Cybersecurity Awareness Training," ISACA Journal, vol. 2, Mar. 2023. [Online]. Available: <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training>
- [7] Andria dan M. Lenawati, "Peningkatan Kesadaran Keamanan Siber melalui Bimbingan Teknis bagi CSIRT dan Tim TIK pada OPD dan BUMD Kabupaten Madiun," in Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (Senatib), Universitas Duta Bangsa Surakarta, 2025.
- [8] E. Nugroho dan A. D. Widianoro, "Teacher Digital Literacy Based on the Pillars of Skill, Ethics, Safety, and Culture," Smart Classroom Digest, vol. 2, no. 2, Des. 2024.
- [9] O. Abrahams et al., "Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability," ResearchGate, Jan. 2024. doi: 10.13140/RG.2.2.26743.27046.
- [10] Badan Siber dan Sandi Negara, "Panduan Pembentukan dan Pengelolaan Tim Tanggap Insiden Siber (CSIRT/TTIS) Pemerintahan Daerah," BSSN, Jakarta, 2022.
- [11] Dinas Komunikasi dan Informatika Provinsi Jawa Timur, "Delapan Daerah di Jatim Sudah Bentuk CSIRT," Jatim Newsroom, Feb. 2025. [Online]. Available: <https://kominfo.jatimprov.go.id>
- [12] A. Fadhil dan S. Yazid, "Measurement of Employee Information Security Awareness: A Case Study of National Civil Service Agency," Indonesian Journal of Computer Science, vol. 12, no. 6, pp. 3581-3597, 2023. doi: 10.33022/ijcs.v12i6.3640.
- [13] M. Bumbungan, M. Yuniar, dan B. Prasetyo, "Peran CSIRT: Strategi Efektif Pencegahan dan Penanganan Insiden Keamanan Siber," Jurnal Keamanan Siber Indonesia, vol. 2, no. 1, 2024.
- [14] D. Fajriyani et al., "Tantangan Kompetensi SDM dalam Menghadapi Era Digital (Literatur Review)," Jurnal Ekonomi Manajemen Sistem Informasi, vol. 5, no. 3, pp. 547-560, 2024.

