Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 11, No. 5, Oktober 2025, hlm. 1057-1072 e-ISSN: 2528-6579

SCENE-CSIRT (EVALUASI KOMPETENSI BERBASIS SKENARIO UNTUK TTIS)

Faizal Wahyu Romadhon*[1], Muhammad Salman[2]

[1,2]Universitas Indonesia, Depok
Email: [1]faizal.wahyu@ui.ac.id, [2]muhammad.salman@ui.ac.id
*Penulis Korespondensi

(Naskah masuk: 6 Februari 2025, diterima untuk diterbitkan: 29 Oktober 2025)

Abstrak

Tim Tanggap Insiden Siber (TTIS) merupakan tim yang bertanggung jawab untuk melaksanakan berbagai fungsi manajemen insiden, seperti deteksi, triase, analisis, dan respons insiden. Namun, dengan meningkatnya kompleksitas ancaman siber serta adanya kesenjangan kompetensi pada TTIS terutama di tingkat pemerintah daerah, diperlukan model evaluasi yang dapat menilai kesiapan personel secara komprehensif. Model SCENE-CSIRT (Evaluasi Kompetensi Berbasis Skenario untuk TTIS) merupakan model yang dikembangkan dengan mengintegrasikan kerangka regulasi nasional (Peraturan yang ada di Indonesia, Peta Okupasi BSSN) dengan standar internasional (NIST, FIRST, NICE *Framework*), sehingga relevan untuk konteks lokal maupun global. Pendekatan ini belum pernah dilakukan sebelumnya dalam konteks evaluasi TTIS di Indonesia. Selain itu, pendekatan berbasis skenario digunakan untuk mengevaluasi keterampilan teknis, seperti analisis insiden dan mitigasi, serta keterampilan non-teknis, seperti komunikasi dan koordinasi. Dengan model evaluasi yang telah disusun diharapkan dapat mengidentifikasi kesenjangan kompetensi serta memberikan rekomendasi pengembangan yang terarah guna meningkatkan efektivitas TTIS. Hasil validasi menunjukkan 97.7% ahli menyetujui model ini dengan mencakup aspek-aspek yang dibutuhkan oleh personel TTIS dalam menangani insiden siber. Penelitian ini diharapkan dapat menjadi acuan dalam pengembangan kebijakan dan penguatan kapasitas TTIS di pemerintah daerah, sehingga meningkatkan kesiapan dan ketangguhan dalam mengelola insiden siber secara efektif.

Kata kunci: *Tim Tanggap Insiden Siber (TTIS), Model Evaluasi Kompetensi, Pemerintah Daerah, Keterampilan Teknis dan Non-teknis, Pemetaan Kompetensi, Pendekatan Berbasis Skenario*

SCENE-CSIRT (*SCENARIO-BASED EVALUATION COMPETENCY FOR* CSIRT)

Abstract

Computer Incident Response Team (CSIRT) is responsible for carrying out various incident management functions, such as detection, triage, analysis, and response. However, with the increasing complexity of cyber threats and existing competency gaps within CSIRTs—particularly at the local government level—there is a need for an evaluation model that can comprehensively assess personnel readiness. The SCENE-CSIRT model (Scenario-Based Competency Evaluation for CSIRT) was developed by integrating national regulatory frameworks (including existing Indonesian regulations and the BSSN Occupational Map) with international standards (such as NIST, FIRST, and the NICE Framework), making it relevant to both local and global contexts. This integrated approach has not been previously applied in the context of CSIRT evaluation in Indonesia. Furthermore, the scenario-based approach is used to evaluate both technical skills (such as incident analysis and mitigation) and non-technical skills (such as communication and coordination). The model is designed to identify competency gaps and provide targeted development recommendations to improve the effectiveness of CSIRTs. Validation results indicate that 97.7% of experts agree that the model encompasses the necessary aspects required by CSIRT personnel in managing cyber incidents. This study is expected to serve as a reference for policy development and capacity building for CSIRTs at the local government level, thereby enhancing preparedness and resilience in managing cyber incidents effectively.

Keywords: *Computer Security Incident Response Team (CSIRT), Competency Evaluation Model, Local Government, Technical and Non-technical Skills, Competency Mapping, Scenario-Based Approach*

1. PENDAHULUAN

Dalam era digital saat ini, teknologi informasi dan komunikasi telah menjadi bagian yang tidak terpisahkan dari hampir semua aspek kehidupan. Namun, seiring dengan perkembangan teknologi, ancaman siber juga semakin berkembang dan

menjadi semakin kompleks. Salah satu risiko ancaman siber yang dapat merugikan organisasi adalah risiko kebocoran data (Gebremeskel, Jonathan and Yalew, 2023). Untuk menghadapi ancaman risiko tersebut, Badan Siber dan Sandi Negara (BSSN) telah menginisiasi pembentukan Tim Tanggap Insiden Siber (TTIS) (Presiden Republik Indonesia, 2019). Hal tersebut memiliki tujuan untuk mengurangi insiden siber yang mungkin terjadi di Indonesia.

Saat ini, telah terbentuk 34 TTIS di pemerintah daerah untuk menghadapi ancaman dan insiden siber. Namun, berdasarkan hasil pemantauan dari BSSN, masih ditemukan beberapa insiden siber seperti kebocoran data dan *web defacement* (BSSN, 2025). Dengan sektor yang paling terdampak adalah sektor administrasi pemerintahan. Hal ini mengindikasikan bahwa TTIS di pemerintahan termasuk pemerintah daerah masih belum berjalan secara optimal untuk mengatasi ancaman dan insiden siber.

TTIS yang dibentuk memiliki tugas dan fungsi yang kompleks dalam mengelola insiden keamanan siber. Salah satu faktor utama yang mempengaruhi efektivitas TTIS adalah kompetensi sumber daya manusia (SDM) yang dimiliki (FIRST, 2019). Sektor pemerintah daerah sering kali menghadapi kendala terkait keterbatasan SDM yang memiliki kompetensi khusus di bidang keamanan siber (Norris, Joshi and Finin, 2015; Prabaswari, Alfikri and Ahmad, 2022; Salwa, 2024). Selain itu berdasarkan laporan dari organisasi internasional, salah satu faktor utama yang berpengaruh terhadap adanya insiden terutama kebocoran data yaitu personel IT yang tidak memiliki keterampilan terkait sehingga dapat menjadi celah yang dapat dimanfaatkan oleh pelaku ancaman (Fortinet, 2024). Oleh karena itu, perlu untuk mengoptimalkan kinerja dari TTIS di pemerintah daerah dimana personel TTIS tersebut harus memiliki keterampilan dan pengalaman yang diperlukan untuk mendeteksi, merespons, dan memitigasi insiden siber secara efektif (BSSN, 2024).

Penelitian ini bertujuan untuk mengembangkan model evaluasi kompetensi personel TTIS yang relevan dan aplikatif dalam konteks Indonesia, dengan fokus khusus pada sektor pemerintah daerah. Hasil dari model ini diharapkan dapat menjadi acuan utama dalam meningkatkan efektivitas TTIS dan dalam memperkuat kemampuan mereka untuk mengelola insiden keamanan siber secara lebih baik. Untuk dapat mengoptimalkan kinerja TTIS, diperlukan adanya evaluasi kompetensi personel TTIS. Evaluasi kompetensi personel TTIS menjadi krusial untuk mengidentifikasi kesenjangan keterampilan dan memastikan kesiapan tim keamanan siber dalam menghadapi ancaman yang terus berkembang (GFCE, 2019). Dengan evaluasi yang tepat, dapat dilakukan pelatihan dan pengembangan kemampuan yang sesuai untuk meningkatkan efektivitas TTIS, sehingga mempercepat penanganan insiden dan memperkecil dampak serangan sehingga tidak meluas. Oleh karena itu, pada penelitian ini akan dikembangkan model untuk melakukan evaluasi kompetensi personel TTIS serta model tersebut relevan untuk digunakan dalam melakukan evaluasi berbasis skenario.

Penelitian ini akan terbagi menjadi beberapa tahapan. Tahapan yang pertama yaitu perancangan model evaluasi kompetensi personel TTIS. Hasil dari model ini akan dievaluasi oleh pakar sehingga hasil yang didapatkan dapat menjadi acuan utama dalam pelaksanaan evaluasi personel TTIS di Indonesia, terutama pada pemerintah daerah.

2. PENELITIAN TERKAIT

2.1. Tim Tanggap Insiden Siber (TTIS)

Manajemen insiden merupakan proses untuk untuk mengenali, menganalisis, dan merespons insiden. Menurut CMU(Alberts et al., 2004a), insiden manajemen sangat luas tidak hanya mencakup penanganan insiden, tapi juga termasuk penanganan kerentanan, penanganan artefak dan pelatihan kesadaran keamanan. Berkaitan dengan hal tersebut TTIS berperan sangat penting dalam proses manajemen insiden tersebut. TTIS akan menjadi entitas utama dalam mengelola dan merespons insiden keamanan siber. TTIS bertanggung jawab untuk melaksanakan berbagai fungsi yang termasuk dalam manajemen insiden, seperti deteksi, triase, analisis, dan respons insiden.

Dalam pelaksanaan manajemen insiden di Indonesia, terdapat kewajiban untuk setiap organisasi di sektor strategis dan penyedia infrastruktur kritis untuk membentuk TTIS (BSSN, 2024). TTIS yang dibentuk memiliki tugas utama yaitu pelaksanaan penanganan insiden siber dari tahap awal sampai dengan diseminasi (Martin et al., 2021). Selain itu menurut FIRST bahwa setiap TTIS yang dibentuk harus memiliki beberapa layanan, dan salah satu layanan utama yaitu *Information Security Incident Management* (FIRST, 2019b). Layanan ini berfokus pada proses dan praktik yang diperlukan untuk mengelola insiden keamanan informasi secara efektif. Hal ini juga dijabarkan melalui beberapa standar ataupun prosedur terkait dengan penanganan insiden (Nelson et al., 2025). Sehingga dapat dijabarkan tugas utama dari TTIS mencakup pelaporan dan penerimaan laporan insiden, penanganan insiden, dan diseminasi insiden. Penelitian dari NICE menyediakan kerangka kerja yang komprehensif dalam pendidikan, pelatihan, dan pengembangan tenaga kerja di bidang keamanan siber (Petersen et al., 2020a). Salah satu peran kerja yang didefinisikan dalam *framework* NICE, khususnya dalam kategori *Protect and Defend* di bidang keamanan siber adalah *Cyber Defense Incident Responder* (PR-CIR-001). Peran ini berfokus pada respons terhadap insiden keamanan dan ancaman yang muncul di lingkungan digital, serta memastikan mitigasi, pemulihan, dan pemahaman menyeluruh terhadap insiden tersebut. Berdasarkan penjabaran tersebut akan menjadi

pelengkap dari penelitian sebelumnya yang sudah ada, sehingga dapat menjabarkan aktivitas yang dilaksanakan oleh TTIS yang lebih menyeluruh.

Berkaitan dengan tugas dari TTIS yang sangat krusial terutama dalam hal penanganan insiden siber, personel yang bertugas harus memiliki keterampilan yang baik. Karena selain aspek manusia menjadi risiko keamanan sendiri, juga menunjukkan bahwa organisasi mungkin kurang siap untuk menangani insiden jika tidak memiliki personel yang kompeten (Furnell, 2021). Penelitian dari CMU menjabarkan bawah TTIS harus memiki keterampilan dasar dan keterampilan teknis (Software Engineering Institute, 2017). Keterampilan dasar tersebut berkaitan dengan tugas dari TTIS yang akan banyak berkomunikasi dengan pihak lain seperti konstituen dari TTIS ataupun pihak lainnya sehingga aspek seperti komunikasi menjadi hal yang harus dimiliki oleh seorang personel TTIS. Sedangkan keterampilan teknis pasti diperlukan mempercepat proses dari penanganan insiden itu sendiri, aspek pengetahuan dasar sangat dibutuhkan dalam hal ini. Jika keterampilan tersebut sudah dikuasai maka TTIS akan dapat melakukan penanganan insiden yang lebih efektif dan efisien sehingga dapat meminimalkan dampak yang lebih luas.

2.2. Model Evaluasi Kompetensi Tim TTIS

Penelitian terkait dengan evaluasi kompetensi dalam keamanan siber telah banyak dilakukan, namun fokusnya bervariasi berdasarkan area spesifik yang diinvestigasi. Berdasarkan penelitian oleh Hranicky dkk. telah mengembangkan peta keterampilan (*skill map*) yang berfokus pada pelatihan profesional *Digital Forensics and Incident Response* (DFIR) (Hranický et al., 2021). Namun, penelitian tersebut kurang menyoroti aspek non-teknis yang juga penting dalam peran TTIS, seperti komunikasi dan koordinasi antar tim.

Penerapan di negara lain terkait dengan evaluasi TTIS tidak spesifik dijabarkan, namun terdapat beberapa pendekatan untuk mengevaluasi TTIS secara organisasi, seperti pendekatan dengan menggunakan SIM3 (Stikvoort, Kossakowski and Maj, 2023) yang menjadi acuan dari ENISA yang berlaku di negara Uni Eropa dan CREST (CREST, 2014) yang juga menjadi acuan oleh BSSN di Indonesia. Selain itu standar lainnya yang mengevaluasi keamanan siber yang lebih menyeluruh termasuk aspek penanganan insiden seperti instrumen Indeks KAMI Versi 5 (BSSN, 2023), NIST CSF (NIST, 2024) dan C2M2 (U.S Department of Energy, 2022) juga tidak secara langsung mengevaluasi personil TTIS. Berdasarkan penjabaran tersebut menunjukkan sebagian besar berfokus pada evaluasi organisasi dan tidak spesifik dalam melakukan evaluasi individu atau personel TTIS itu sendiri. Sehingga perlu adanya model yang secara khusus dapat digunakan untuk melakukan evaluasi personel TTIS.

Penelitian oleh Ghos dan Francia mengeksplorasi penggunaan skenario *based learning* dalam evaluasi kompetensi personel keamanan siber (Ghosh and Francia, 2021). Pada penelitian lainnya menggunakan metode tersebut untuk meningkatkan kemampuan personel organisasi dalam hal penanganan insiden siber. Selain itu, model pembelajaran berbasis skenario juga digunakan oleh Alothman dkk. (Alothman et al., 2022)untuk mengukur efektivitas tim keamanan, baik itu dalam peran *blue team* maupun *red team*.

Tabel 1. Pemetaan Peta Okupasi terhadap Tugas TTIS

No	Nama Okupasi	Deskripsi
1	*Cybersecurity Operator*	Mengidentifikasi kerawanan dan menjalankan prosedur keamanan siber di SOC sesuai instruksi.
2	*Junior Cybersecurity*	Melaksanakan implementasi program keamanan siber sesuai tugas.
3	*Cybersecurity Administrator*	Mengimplementasikan dan melaporkan pelaksanaan program keamanan siber berdasarkan manajemen risiko.
4	*Digital Evidence First Responder*	Merespons insiden siber dan memeriksa barang bukti elektronik secara awal.
5	*Cybersecurity Analyst / Cybersecurity Incident Analyst*	Menganalisis insiden, memantau ancaman, serta menindaklanjuti tiket insiden di SOC.
6	*Incident Response Team Manager*	Mengelola penanganan insiden dan ancaman siber serta menyediakan koordinasi dan komunikasi.
7	*Digital Forensic Analyst*	Memeriksa bukti digital secara mendalam untuk investigasi dan persidangan kasus *cybercrime*.
8	*Cyber Forensic Specialist*	Menganalisis bukti digital dari jaringan untuk investigasi dan penuntutan *cybercrime*.
9	*Cyber Incident Investigarion Manager*	Mengelola sumber daya investigasi insiden siber secara teknis, ilmiah, dan legal.

Penelitian oleh Koutsouris dkk. telah mengembangkan matriks yang dapat digunakan untuk menilai kinerja pelatihan keamanan siber (Koutsouris, Vassilakis and Kolokotronis, 2021). Berdasarkan beberapa penelitian yang sudah ada, menunjukkan bahwa model skenario selain digunakan dalam pelatihan juga dapat digunakan dalam evaluasi kemampuan personel. Penelitian lainnya juga telah menjabarkan kemampuan yang harus dimiliki oleh personel TTIS yang terbagi menjadi kemampuan personel, kemampuan teknis dan kemampuan tambahan (Software Engineering Institute, 2017; Villegas-Ch, Ortiz-Garces and Sánchez-Viteri, 2021).

Gambar 1 Tahapan Penelitian

Sehingga untuk dapat melakukan evaluasi personel secara lebih komprehensif akan dilakukan penyusunan model evaluasi yang nantinya akan dapat dijabarkan pada model evaluasi berbasis skenario.

Metode berbasis skenario sendiri merupakan metode pelatihan yang umumnya digunakan dalam simulasi situasi nyata untuk mempersiapkan tim respons insiden dalam menghadapi ancaman keamanan siber (Angafor, Yevseyeva and Maglaras, 2023). Model ini memungkinkan evaluasi yang lebih kontekstual dan situasional, yang relevan untuk tugas yang dihadapi oleh anggota TTIS. Hal tersebut diharapkan dapat mengukur atau mengetahui kemampuan dari personel dari masing masing tim TTIS di sektor pemerintah daerah berdasarkan kasus nyata.

Di Indonesia, tersedia dokumen yang memetakan okupasi bidang keamanan siber yaitu Peta Okupasi Keamanan Siber (BSSN, 2019). Dokumen tersebut mencakup standar kompetensi dengan rincian spesifik keterampilan dan pengetahuan yang diperlukan di bidang keamanan siber. Tabel 1 menampilkan pemetaan okupasi dalam area fungsi keamanan siber yang berhubungan dengan tugas dari personel TTIS. Berdasarkan tabel tersebut, terdapat 9 okupasi terkait tugas TTIS, masing-masing dengan level kompetensi yang dapat digunakan untuk menyusun rekomendasi aktivitas tugas TTIS.

3. METODE PENELITIAN

SCENE-CSIRT (Evaluasi Kompetensi Berbasis Skenario untuk TTIS) yang disusun merupakan model yang dapat digunakan dalam menilai dan menganalisis kemampuan personel TTIS. Model tersebut menggabungkan kerangka regulasi nasional yaitu Peraturan BSSN No 1 Tahun 2024 terkait Tim Tanggap Insiden Siber (BSSN, 2024) dan Peta Okupasi Nasional (BSSN, 2019) yang digabungkan dengan standar internasional yaitu kerangka dari, kerangka kerja dari NICE dan standar dari NIST terkait dengan penanganan insiden siber (Nelson et al., 2025). Sehingga dengan adanya acuan tersebut model yang disusun relevan untuk konteks lokal maupun secara global. Selain itu, pendekatan ini belum pernah dilakukan sebelumnya dalam konteks evaluasi TTIS di Indonesia. Model ini membantu dalam mengidentifikasi kelebihan dan kekurangan setiap TTIS yang ada, serta memberikan masukan untuk peningkatan kompetensi selanjutnya. Untuk menyusun model tersebut terbagi menjadi beberapa tahapan penelitian seperti pada Gambar 1.

3.1. Pemetaan Kompetensi TTIS

Pada tahap ini, kami melakukan identifikasi keterampilan yang dibutuhkan berdasarkan pemetaan kompetensi yang telah disusun, dengan tujuan untuk merumuskan keterampilan spesifik yang diperlukan oleh personel TTIS di lingkungan pemerintah daerah. Pemetaan ini mencakup tugas dari TTIS yang dijabarkan dalam setiap aktivitasnya. Selain itu, dalam merumuskan keterampilan ini, kami menjadikan regulasi yang ada di Indonesia sebagai rujukan utama, khususnya regulasi terkait pengelolaan insiden siber dari BSSN (BSSN, 2024). Regulasi ini menggambarkan tahapan proses pengelolaan insiden yang diterapkan di Indonesia, sehingga menjadi acuan yang relevan dan kontekstual bagi peran TTIS dalam pemerintahan daerah.

Selain mengacu pada regulasi di Indonesia, kami juga melengkapi pemetaan kompetensi dengan mengacu pada beberapa kerangka kerja yang sudah ada seperti dari *Forum of Incident Response and Security Teams* (FIRST) (FIRST, 2019b) dan *National Initiative for Cybersecurity Education* (NICE) *Framework* (Petersen et al., 2020a). Kerangka dari FIRST menjabarkan standar dan panduan dalam menangani insiden keamanan siber, sedangkan NICE *Framework* menyediakan klasifikasi dan deskripsi peran serta keterampilan di berbagai domain keamanan siber. Pada tahapan ini kami juga mengacu pada standar internasional untuk siklus penanganan insiden seperti standar dari NIST yang memberikan panduan yang komprehensif mulai dari persiapan, deteksi, analisis, hingga mitigasi insiden (Nelson et al., 2025). Dengan memadukan regulasi nasional dan standar internasional ini, kami dapat mengidentifikasi berbagai keterampilan penting yang diperlukan personel TTIS, termasuk kemampuan teknis seperti analisis dan mitigasi insiden, serta keterampilan non-teknis seperti koordinasi dan komunikasi yang diperlukan dalam pengelolaan insiden siber secara efektif di lingkungan pemerintah daerah.

3.2. Penyusunan Rubrik Evaluasi Kompetensi TTIS

Pada tahap ini, kami menyusun rubrik evaluasi kompetensi TTIS dengan menguraikan tingkatan kemampuan berdasarkan Peta Okupasi Nasional Area Fungsi Keamanan Siber (BSSN, 2019) dan beberapa pelatihan terkait. Pendekatan tersebut digunakan untuk memetakan setiap aktivitas berada ditingkat tertentu, sehingga akan mempermudah dalam pemetaan rekomendasi pengembangan kompetensi. Selain itu, pada tahapan ini, kami juga memastikan bahwa setiap tugas yang dijalankan TTIS dapat dikategorikan pada tingkat tertentu yang akan mempermudah dalam memberikan rekomendasi untuk pengembangan kompetensi personel di masa mendatang. Pada tahapan ini, kami juga menyusun daftar pertanyaan dan artifak yang dapat digunakan dalam mengevaluasi kompetensi personel TTIS. Selain itu, untuk pendekatan berbasis skenario, kami menggunakan data insiden yang terjadi di sektor pemerintah daerah sehingga pertanyaan dan artifak relevan digunakan untuk evaluasi personel TTIS di pemerintah daerah.

3.5. Validasi Model

Untuk memverifikasi model SCENE-CSIRT yang dikembangkan, penelitian ini menggunakan metode *expert judgement* berbentuk kuesioner. Tahapan awal adalah menyusun kuesioner yang dirancang untuk menilai keterkaitan antara pemetaan tugas, rubrik evaluasi kompetensi, skenario yang dikembangkan, dan pertanyaan yang digunakan untuk evaluasi.

Kuesioner ini terdiri dari dua bagian. Bagian pertama berfokus pada pemetaan tugas dan fungsi, mengevaluasi kesesuaian antara tugas yang dipetakan dengan fungsi TTIS serta keterkaitan tugas tersebut dengan kompetensi yang dibutuhkan. Sedangkan bagian kedua bertujuan untuk mengukur kelengkapan dan kejelasan rubrik evaluasi kompetensi.

Sebanyak enam ahli dilibatkan dalam proses penilaian. Para ahli ini dipilih berdasarkan pengalaman mereka dalam terkait dengan TTIS. Tahapan validasi dimulai dengan penyebaran kuesioner kepada para ahli, diikuti dengan pengumpulan umpan balik untuk dievaluasi dan diringkas. Hasil dari kuisoner tersebut masing-masing pertanyaan diolah dengan menghitung tingkat kesepakatan dari masing-masing pertanyaan. Sehingga didapatkan presentasi kesepakatan secara keseluruhan model yang telah disusun. Hasil validasi ini memberikan wawasan berharga yang digunakan untuk memperbaiki dan menyempurnakan model evaluasi. Dengan demikian, model evaluasi yang dihasilkan menjadi lebih valid dan dapat digunakan untuk mengukur keterampilan TTIS secara komprehensif, serta sesuai dengan kebutuhan operasional TTIS.

4. HASIL DAN PEMBAHASAN

4.1. Pemetaan Tugas dan Kompetensi TTIS

Pada tahapan ini kami telah memetakan tugas dari TTIS dengan memetakan dari regulasi yang sudah ada yaitu Peraturan BSSN No 1 Tahun 2024 (BSSN, 2024) yang dilengkapi dengan kerangka kerja dari FIRST (FIRST, 2019b) dan NICE (Petersen et al., 2020a). Kami juga memetakan aktivitas dan tugas yang ada berdasarkan tahapan manajemen insiden yang telah dijabarkan oleh *Carnegie Mellon University* (Alberts et al., 2004b) dan standar dari NIST terkait dengan penanganan insiden siber (Nelson et al., 2025). Berikut merupakan penjabaran keseluruhan aktivitas tugas dan aktivitas dari TTIS yang terlihat pada Tabel 2.

Tabel 2. Pemetaan Tugas TTIS

No	Tahapan Manajemen Insiden	Tugas	Aktivitas
1	Perencanaan dan Persiapan	Pengembangan Rencana Tanggap	Membuat rencana tanggap insiden yang komprehensif
		Pelatihan Personel	Melatih personel secara berkala dalam menghadapi insiden siber
		Pemahaman Peran	Memastikan setiap personel memahami perannya
2	Deteksi dan Analisis	Deteksi Insiden	Mendeteksi adanya insiden
		Pengumpulan Informasi	Mengumpulkan informasi internal dan eksternal
		Pelaporan Konstituen	Menerima dan menindaklanjuti laporan insiden dari konstituen
3	Klasifikasi dan Prioritas	Penentuan Tingkat Urgensi	Menentukan tingkat urgensi insiden
		Penentuan Dampak	Menilai dampak insiden
4	Respons Insiden	Isolasi Insiden	Melakukan isolasi untuk meminimalkan kerugian lebih lanjut
		Mitigasi Insiden	Melakukan mitigasi sesuai rencana tanggap insiden
		Penerapan Pertahanan Berlapis	Menerapkan pertahanan untuk mencegah penyebaran insiden
5	Pengumpulan Bukti dan Investigasi	Pengumpulan Bukti Digital	Mengumpulkan bukti digital dari berbagai sumber
		Analisis Bukti	Menganalisis bukti untuk memahami akar masalah

		Korelasi Antar Insiden	Menganalisis log file dan mengkorelasikan insiden terkait
6	Eradikasi dan Pemulihan	Penghapusan Ancaman	Menghilangkan file mencurigakan yang terkait ancaman
		Pemulihan Sistem	Memulihkan sistem ke kondisi normal setelah ancaman dihapus
7	Komunikasi dan Pelaporan	Pelaporan kepada Pihak Terkait	Memberikan informasi ke media, penegak hukum, dan pihak terkait lainnya
		Pelaporan ke TTIS Tingkat Atas	Melaporkan insiden ke TTIS Sektor atau TTIS Nasional sesuai regulasi
8	Evaluasi dan Pembelajaran	Evaluasi Efektivitas Respons	Meninjau efektivitas respons yang telah dilakukan
		Pembagian Informasi	Membagikan informasi insiden dan detail penanganan dengan konstituen dan TTIS lainnya

Berdasarkan pemetaan tugas dari TTIS pada Tabel 2. Tabel yang disusun mencakup tahapan-tahapan penting dalam manajemen insiden siber yang dilakukan oleh TTIS. Pada tabel tersebut terbagi menjadi beberapa bagian yaitu tahap manajemen insiden, tugas, dan aktivitas dari TTIS. Tahap manajemen insiden menggambarkan langkah-langkah sistematis yang perlu diambil untuk menangani insiden siber secara efektif dari sebelum, saat dan setelah insiden. Berikut ini merupakan generalisasi penjabaran tugas dari TTIS yang telah disusun :

a) Tahapan Perencanaan dan Persiapan
Pada tahapan ini TTIS mengembangkan rencana tanggap insiden yang komprehensif dan memastikan bahwa semua personel memahami perannya (BSSN, 2024). Selain itu pada tahapan ini juga setiap personel harus terus dilatih dalam menghadapi insiden siber, sehingga personel selalu dalam kondisi siap untuk menghadapi insiden siber.

b) Tahapan Deteksi dan Analisis
Pada tahap deteksi dan analisis, TTIS berfokus pada mendeteksi adanya insiden serta mengumpulkan informasi yang relevan untuk memahami akar masalahnya. Pengumpulan informasi tidak hanya pada dari sumber internal tapi juga dari sumber data eksternal seperti data *threat intelligence* (Petersen et al., 2020b). Selain itu pada tahapan ini TTIS juga akan menerima laporan dari konstituen TTIS yang harus ditindaklanjut (FIRST, 2019b).

c) Tahapan Klasifikasi dan Prioritas
Tahapan selanjutnya setelah laporan diterima dan dinyatakan sebagai sebuah insiden, tahap klasifikasi dan prioritas dilakukan untuk menentukan tingkat urgensi dan dampak dari insiden tersebut (FIRST, 2019b; Petersen et al., 2020b; BSSN, 2024). Selain itu dengan tahapan klasifikasi dan prioritas ini dapat membantu tim untuk merespons dengan cepat dan efisien terhadap sebuah insiden.

d) Tahapan Respons Insiden
Pada tahap respons insiden, tindakan seperti isolasi dan mitigasi insiden dilakukan untuk meminimalkan kerugian lebih lanjut (BSSN, 2024). Hal ini bisa dilakukan dengan mengikuti rencana tanggap insiden yang telah dibuat, dengan mengikuti rencana tanggap insiden yang telah ada maka sebagai TTIS bisa menerapkan pertahanan berlapis untuk mencegah insiden tersebut meluas.

e) Tahapan Pengumpulan Bukti dan Investigasi
Pada tahapain ini, setelah insiden ditangani, tahap pengumpulan bukti dan investigasi berlangsung, di mana bukti digital dikumpulkan dan dianalisis untuk memahami bagaimana insiden terjadi dan untuk mencegah insiden serupa di masa depan (FIRST, 2019b; BSSN, 2024). Pada tahapan ini juga juga akan melakukan korelasi antar insiden termasuk dengan menganalisis *log file* dari berbagai sumber (Petersen et al., 2020b).

f) Tahapan Eradikasi dan Pemulihan
Tahap eradikasi dan pemulihan bertujuan untuk menghilangkan ancaman yang ada dan memulihkan sistem ke kondisi normal (BSSN, 2024). Setelah ditemukan akar masalah dan pengumpulan bukti telah dilakukan, pada tahapan ini TTIS dapat melakukan penghapusan *file* yang mencurigakan sehingga sistem bisa kembali normal.

g) Tahapan Komunikasi dan Pelaporan
Tahap komunikasi dan pelaporan penting untuk memastikan bahwa semua pihak (media, penegak hukum, pihak lainnya) terkait mendapatkan informasi yang tepat tentang insiden. Termasuk jika perlu untuk berhubungan dengan personel penegak hukum maka TTIS dapat memberikan informasi detail insiden sesuai dengan kebutuhan (Petersen et al., 2020b). Selain itu berdasarkan regulasi di Indonesia, maka TTIS wajib untuk melaporkan ke TTIS diatasnya seperti TTIS Sektor ataupun TTIS Nasional (BSSN, 2024).

h) Tahapan Evaluasi dan Pembelajaran

Pada tahapan evaluasi dan pembelajaran dilakukan untuk meninjau efektivitas respons yang telah dilakukan serta untuk memperbaiki proses di masa yang akan datang. Selain itu untuk pembelajaran maka TTIS harus membagikan informasi insiden dan detail penanganan terhadap konstituennya ataupun pihak TTIS lainnya (FIRST, 2019b; Petersen et al., 2020b; BSSN, 2024).

Secara keseluruhan, pada tabel yang telah disusun menjabarkan tugas menyeluruh dari TTIS. Dengan memetakan tahapan, sub-tugas, dan aktivitas secara jelas, TTIS dapat memastikan bahwa proses penanganan insiden dilakukan secara sistematis dan efisien.

4.2. Penyusunan Evaluasi Rubrik Kompetensi

Setelah tugas dari TTIS terpetakan secara keseluruhan, selanjutnya kami menyusun rubrik evaluasi kompetensi. Rubrik tersebut akan digunakan untuk menilai atau mengukur kemampuan personel TTIS berdasarkan beberapa indikator yang telah ditetapkan. Rubrik ini diadaptasi berdasarkan Peta Okupasi Nasional Area Fungsi Keamanan Siber (BSSN, 2019) dan pelatihan terkait dari SANS, FIRST, ISC2 dan EC-Council untuk bisa mengidentifikasi secara menyeluruh setiap aktivitas berada di tingkatan apa. Selanjutnya, kami telah menjabarkan aktivitas yang dipetakan menjadi tiga tingkatan untuk rubrik evaluasi kompetensi yaitu belum memadai (*unsatisfactory*), sedang berkembang (*developing*), dan memadai (*satisfactory*) (Northern Illinois University Center for Innovative Teaching and Learning, 2012). Pada Tabel 3 merupakan hasil pemetaan tingkat kompetensi TTIS berdasarkan ativitasnya.

Tabel 3. Pemetaan Rubrik Evaluasi Kompetensi TTIS

No	Indikator	Tingkat Okupasi	Tingkatan Kompetensi			Pelatihan
			Belum Memadai (Unsatisfactory)	Sedang Berkembang (Developing)	Memadai (Satisfactory)	
1	Mengembangkan dokumen rencana tanggap insiden sesuai dengan standar organisasi	Lanjutan	Belum memahami terkait dengan rencana tanggap insiden siber	Pemahaman sebagian terkait dengan rencana tanggap insiden siber	Pemahaman menyeluruh terkait dengan rencana tanggap insiden untuk bisa menyusun dokumen tersebut	LDR553: *Cyber Incident Management* - SANS
2	Menyusun modul pelatihan dan evaluasi untuk tim respons insiden	Menengah	Belum memahami terkait dengan pelatihan dan evaluasi yang bisa diselenggarakan untuk tim respons insiden	Pemahaman sebagian terkait dengan pelatihan dan evaluasi yang bisa diselenggarakan untuk tim respons insiden	Pemahaman menyeluruh terkait dengan pelatihan dan evaluasi yang bisa diselenggarakan untuk tim respons insiden	*Conducting Exercises to improve Incident Response* - FIRST
3	Menyediakan panduan peran dan tanggung jawab	Dasar	Belum memahami terkait dengan peran dan tanggung jawab dari masing-masing personel di TTIS	Pemahaman sebagian terkait dengan peran dan tanggung jawab dari masing-masing personel di TTIS	Pemahaman menyeluruh terkait dengan peran dan tanggung jawab dari masing-masing personel di TTIS	CSIRT *Basic Course* - FIRST
4	Menggunakan sistem deteksi intrusi dan alat analisis	Menengah	Belum mampu untuk menggunakan sistem deteksi intrusi dan alat analisis seperti SIEM	Mampu sebagian untuk menggunakan sistem deteksi intrusi dan alat analisis seperti SIEM	Dapat menggunakan sistem deteksi intrusi dan alat analisis seperti SIEM secara maksimal	*FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics*- SANS
5	Menjalankan analisis dan komunikasi dengan pihak ketiga	Menengah	Belum memahami terkait dengan tahapan analisis dan komunikasi dengan pihak lainnya	Pemahaman sebagian terkait dengan tahapan analisis dan komunikasi dengan pihak lainnya	Pemahaman menyeluruh terkait dengan tahapan analisis dan komunikasi dengan pihak lainnya	*Certified Threat Intelligence Analyst* (CTIA) – EC-Council

No	Indikator	Tingkat Okupasi	Tingkatan Kompetensi			Pelatihan
			Belum Memadai (Unsatisfactory)	Sedang Berkembang (Developing)	Memadai (Satisfactory)	
6	Memverifikasi dan mengklasifikasikan laporan insiden	Dasar	Belum mampu untuk memverifikasi dan mengklasifikasikan laporan insiden	Mampu sebagian untuk memverifikasi dan mengklasifikasikan laporan insiden	Dapat memverifikasi dan mengklasifikasikan laporan insiden secara detil	CSIRT *Basic Course* - FIRST
7	Melakukan analisis dampak dan menetapkan prioritas respons	Menengah	Belum mampu untuk melakukan analisis dampak dan menetapkan prioritas respons	Mampu sebagian untuk melakukan analisis dampak dan menetapkan prioritas respons	Dapat melakukan analisis dampak dan menetapkan prioritas respons secara detil	*Cybersecurity Administrator* - Peta Okupasi dan SEC504*: Hacker Tools, Techniques, and Incident Handling* - SANS
8	Menggunakan kerangka kerja untuk evaluasi dampak insiden	Lanjutan	Belum mampu untuk menggunakan kerangka kerja untuk evaluasi dampak insiden	Mampu sebagian untuk menggunakan kerangka kerja untuk evaluasi dampak insiden	Dapat menggunakan kerangka kerja untuk evaluasi dampak insiden secara detil	*Cybersecurity Administrator* - Peta Okupasi dan SEC504*: Hacker Tools, Techniques, and Incident Handling* - SANS
9	Koordinasi penanganan insiden dan manajemen krisis	Lanjutan	Belum memahami pihak-pihak yang dapat di koordinasikan terkait sebuah insiden	Memahami sebagian pihak-pihak yang dapat di koordinasikan terkait sebuah insiden	Memahami secara menyeluruh pihak-pihak yang dapat di koordinasikan terkait sebuah insiden	*Cybersecurity Analyst / Cybersecurity Incident Analyst* dan LDR553: *Cyber Incident Management* - SANS
10	Berkoordinasi dengan penegakan hukum selama insiden keamanan	Lanjutan	Belum memahami terkait perlunya koordinasi dengan penegakan hukum selama insiden keamanan	Memahami sebagian terkait perlunya koordinasi dengan penegakan hukum selama insiden keamanan	Memahami secara menyeluruh koordinasi dengan penegakan hukum selama insiden keamanan	*Incident Response Team Manager* - Peta Okupasi dan LDR553: *Cyber Incident Management* - SANS
11	Mengidentifikasi dan melokalisir serangan siber	Menengah	Belum mampu untuk mengidentifikasi adanya serangan siber	Mampu sebagian untuk mengidentifikasi serangan siber untuk dilakukan lokalisir terkait perangkat terdampak	Mampu mengidentifikasi serangan siber secara menyeluruh untuk dilakukan lokalisir terkait perangkat terdampak	*Digital Evidence First Responder* - Peta Okupasi
12	Menggunakan teknik pertahanan siber	Menengah	Belum mampu memahami cara perlindungan terhadap sebuah aset	Mampu untuk melakukan perlindungan terhadap sebuah aset	Mampu untuk melakukan perlindungan terhadap sebuah aset	*Digital Forensics and Incident Response* (DFIR) - SANS *Institute*
13	Melakukan preservasi dan akuisisi barang bukti elektronik dan digital	Menengah	Belum dapat melakukan preservasi dan akuisisi barang bukti elektronik dan digital	Mampu sebagian untuk dapat melakukan preservasi dan akuisisi barang bukti elektronik dan digital	Mampu untuk melakukan preservasi dan akuisisi barang bukti elektronik dan digital sesuai dengan prosedur	*Digital Evidence First Responder* dan FOR498: *Digital Acquisition and Rapid Triage* - SANS
14	Menggunakan teknik analisis forensik untuk mendapatkan data investigatif	Lanjutan	Belum mampu menggunakan teknik analisis forensik untuk mengumpulkan dan menganalisis data investigatif.	Mampu untuk menggunakan beberapa teknik analisis forensik, namun hanya sebagian data yang dianalisis secara menyeluruh dan masih terdapat kelemahan dalam proses tersebut.	Mampu menggunakan teknik analisis forensik secara menyeluruh untuk mengumpulkan, memverifikasi, dan menganalisis data investigatif dengan cara yang sistematis dan detail.	FOR508: *Advanced Incident Response, Threat Hunting, and Digital Forensics*

No	Indikator	Tingkat Okupasi	Tingkatan Kompetensi			Pelatihan
			Belum Memadai (Unsatisfactory)	Sedang Berkembang (Developing)	Memadai (Satisfactory)	
15	Menganalisis *log* dengan alat analisis *log* untuk mengidentifikasi pola dan anomali	Menengah	Belum dapat melakukan analisis *log* untuk mengidentifikasi *root cause* sehingga insiden bisa terjadi.	Mampu untuk melakukan analisis *log* namun belum dapat mengidentifikasi *root cause* sehingga insiden bisa terjadi.	Dapat secara maksimal untuk menganalisis log dan mengidentifikasi *root cause* sehingga insiden bisa terjadi.	*Cyber Forensic Specialist* dan SEC504*: Hacker Tools, Techniques, and Incident Handling* - SANS
16	Melakukan pembersihan sistem berdasarkan kebijakan keamanan	Dasar	Belum mampu untuk mengidentifikasi file berbahaya untuk dilakukan pembersihan	Mampu sebagian untuk mengidentifikasi file berbahaya untuk dilakukan pembersihan	Mampu untuk mengidentifikasi file berbahaya untuk dilakukan pembersihan secara menyeluruh	EC-Council *Certified Incident Handler* (ECIH) - EC-Council
17	Melakukan proses pemulihan dan pengujian sistem untuk memastikan integritas data	Menengah	Belum memahami tahapan pemulihan dan pengujian sistem	Memahami tahapan pemulihan namun belum dapat memastikan data sesuai dengan integritas datanya	Mampu memahami tahapan pemulihan dan pengujian sistem secara maksimal	*Digital Evidence First Responder* - Peta Okupasi dan EC-Council *Disaster Recovery Professional* (EDRP) - EC-Council
18	Mengelola komunikasi krisis dan menyusun laporan insiden	Lanjutan	Tidak memahami struktur komunikasi krisis atau elemen penting dalam laporan insiden.	Memiliki pemahaman tentang elemen komunikasi krisis dasar dan dapat membuat laporan sederhana.	Menguasai teknik komunikasi krisis, termasuk identifikasi stakeholder utama, pesan kunci, dan saluran komunikasi yang tepat.	LDR525: *Managing Cybersecurity Initiatives & Effective Communication*
19	Memberikan testimoni keterangan ahli di persidangan	Lanjutan	Belum mampu untuk melakukan testimoni keterangan ahli di persidangan	Mampu melakukan testimoni tetapi masih memiliki keterbatasan dalam menjelaskan aspek teknis secara jelas dan lengkap	Mampu melakukan testimoni keterangan ahli di persidangan dengan jelas, lugas, dan terperinci, serta menyampaikan informasi teknis dengan mudah dimengerti oleh pengadilan.	*Digital Forensic Analyst* - Peta Okupasi
20	Mengikuti prosedur pelaporan insiden yang ditetapkan oleh regulasi	Menengah	Belum mampu untuk melakukan pelaporan insiden sesuai prosedur yang ditetapkan.	Mampu melakukan pelaporan insiden, tetapi belum sepenuhnya sesuai dengan prosedur yang ditetapkan.	Mampu melakukan pelaporan insiden sesuai dengan prosedur yang ditetapkan secara tepat, lengkap, dan sesuai dengan regulasi yang berlaku.	CSIRT *Basic Course* - FIRST
21	Melakukan evaluasi pasca insiden untuk identifikasi area perbaikan	Lanjutan	Belum mampu melakukan evaluasi pasca insiden untuk mengidentifikasi area perbaikan.	Memahami beberapa bagian dari evaluasi pasca insiden tetapi belum dapat mengidentifikasi area perbaikan dengan jelas.	Dapat melakukan evaluasi pasca insiden dengan efektif untuk mengidentifikasi dan menyarankan area perbaikan yang jelas.	*Incident Response Team Manager* - Peta Okupasi , LDR553: *Cyber Incident Management* - SANS
22	Mengorganisir sesi pembelajaran dan berbagi informasi	Menengah	Belum memahami proses berbagi informasi terkait insiden keamanan.	Memahami sebagian dari proses berbagi informasi, namun belum memahami data spesifik yang perlu dibagikan.	Memahami secara menyeluruh proses berbagi informasi dan memahami data yang perlu dibagikan dalam konteks insiden.	CSIRT *Basic Course* - FIRST

Pada Tabel 3 telah dipetakan indikator, pemetaan okupasi, pemetaan kompetensi dan rekomendasi pelatihan yang akan digunakan pada tahapan evaluasi. Berikut ini merupakan penjabaran dari masing -masing aspek :

a) Indikator

Indikator merujuk pada kriteria yang digunakan untuk menilai kemampuan personel TTIS berdasarkan aktivitas yang telah dijabarkan dalam Tabel 1. Indikator ini mencakup berbagai elemen yang mengukur tingkat keterampilan yang diperlukan untuk menangani insiden siber. Indikator merujuk pada kriteria yang digunakan untuk menilai kemampuan personil TTIS berdasarkan aktivitas yang telah dijabarkan dalam Tabel 2 Tingkat Okupasi merupakan tingkatan keterampilan yang dibutuhkan dalam suatu aktivitas yang telah dijabarkan. Dalam konteks evaluasi kompetensi, pemetaan tingkat keterampilan atau pengetahuan yang diperlukan dalam menjawab pertanyaan tertentu selama evaluasi. Konsep ini digunakan untuk menyesuaikan jenis pertanyaan dan level kesulitan agar sesuai dengan peran atau posisi dalam TTIS. Berikut ini merupakan penjabaran tingkat okupasi, antara lain :

1) Tingkat Dasar: Pada tingkat dasar, personil TTIS harus mampu untuk melakukan tugas-tugas dasar seperti memahami peran dan tanggung jawab dalam tim, menerima dan menindaklanjuti laporan insiden, serta melaksanakan prosedur dasar untuk membersihkan sistem dari ancaman. Keterampilan ini penting untuk memastikan bahwa TTIS dapat menjalankan tugas dengan baik dalam situasi insiden dan mematuhi kebijakan keamanan yang ada.
2) Tingkat Menengah: Pada tingkat menengah, personil TTIS diharapkan memiliki keterampilan analitis yang lebih baik dan kemampuan untuk berkoordinasi dengan tim dan pihak ketiga. Mereka harus mampu melatih anggota tim lainnya, mengumpulkan informasi dari berbagai sumber, serta menentukan tingkat urgensi dan dampak insiden. Keterampilan ini memungkinkan individu untuk merespons insiden secara efektif dan mengambil keputusan yang tepat dalam situasi yang kompleks.
3) Tingkat Lanjutan: Pada tingkat lanjutan, personil TTIS harus memiliki keahlian mendalam dan kemampuan kepemimpinan dalam menangani insiden. Mereka bertanggung jawab untuk mengembangkan rencana tanggap insiden yang komprehensif, memimpin koordinasi penanganan insiden, dan menganalisis bukti untuk mengidentifikasi akar masalah. Keterampilan ini sangat penting untuk mengelola situasi kritis dan memastikan bahwa organisasi dapat pulih dari insiden dengan efektif dan efisien.

b) Pemetaan Kompetensi

Pemetaan kompetensi adalah proses yang menghubungkan keterampilan atau kemampuan yang diperlukan untuk suatu aktivitas dengan tingkat kompetensi yang harus dicapai oleh personil TTIS. Proses ini memastikan bahwa personil TTIS memiliki kemampuan yang sesuai dengan tingkat kompetensi yang ditetapkan untuk setiap aktivitas dalam tahapan manajemen insiden. Dengan demikian, pemetaan ini membantu memastikan bahwa setiap personel dapat menjalankan tugasnya secara efektif dan selaras dengan standar yang diperlukan. Berikut merupakan penjabaran tingkatan pemetaan:

1) *Unsatisfactory* (Tidak Memadai): Personel TTIS belum menunjukkan pemahaman atau kemampuan yang cukup terhadap kompetensi yang diukur. Masih terdapat banyak kekurangan, baik dalam pengetahuan dasar maupun kemampuan praktik.
2) *Developing* (Sedang Berkembang): Personel TTIS telah memiliki pemahaman dasar dan mampu menunjukkan kemampuan praktis dalam beberapa aspek kompetensi, tetapi belum konsisten atau menyeluruh. Masih ada area yang memerlukan pengembangan lebih lanjut.
3) *Satisfactory* (Memadai): Personel TTIS memiliki pemahaman yang baik dan mampu menjalankan tugas terkait kompetensi secara efektif sesuai standar yang ditetapkan. Kemampuan dan pengetahuan sudah dapat diandalkan.

c) Pelatihan

Pelatihan adalah kegiatan yang dirancang untuk mengembangkan keterampilan personel TTIS sesuai dengan indikator yang telah ditetapkan. Dalam konteks ini, pelatihan akan menjadi dasar bagi personel TTIS untuk menguasai keterampilan yang relevan, seperti analisis *log*, penanganan insiden, atau pemulihan dari serangan. Selain itu, berdasarkan hasil evaluasi

kompetensi peserta, ini berfungsi untuk memberi saran tentang program pelatihan lebih lanjut yang harus diikuti untuk mengembangkan atau meningkatkan area keterampilan tertentu yang masih kurang.

Selanjutnya kami menjabarkan pertanyaan dan artifak yang dapat digunakan untuk melakukan evaluasi. Pada penelitian yang telah dijabarkan sebelumnya, metode evaluasi berbasis skenario sangat baik digunakan untuk mengevaluasi personel berdasarkan kondisi nyata. Untuk skenario yang diambil yaitu insiden kebocoran data karena insiden tersebut paling banyak terdampak pada sektor administrasi pemerintahan (BSSN, 2025) . Berikut ini merupakan pemetaan pertanyaan dan sampel artifak untuk skenario kebocoran data berdasarkan tugas TTIS yang telah dijabarkan pada tahapan sebelumnya seperti pada Tabel 4.

Tabel 4. Pemetaan Evaluasi TTIS berdasarkan Skenario Kebocoran Data

Tugas TTIS	Sampel Pertanyaan Evaluasi	Sampel Artifak
Perencanaan dan Persiapan	Dalam dokumen *Incident Response Plan* (IRP) harus dijabarkan langkah yang harus diambil jika insiden kebocoran data yang terdeteksi tidak dapat ditangani oleh tim respons insiden organisasi?	Dokumen *Incident Response Plan* dari CMU (Carnegie Mellon University, 2014)
	Dalam melatih penanganan insiden, kita dapat menggunakan lingkungan komputasi elektronik yang terisolasi dari jaringan langsung, dengan sistem, jaringan, layanan, dan pengguna yang diatur sesuai skenario latihan tertentu, disebut apakah hal tersebut?	Dokumen *Cyber Exercise Playbook* dari MITRE (Jason Kick, 2014)
	Sebuah insiden kebocoran data terjadi di organisasi anda, TTIS wajib menginformasikan ke pihak terdampak. Berdasrkan dokumen dari FIRST termasuk layanan apakah hal tersebut?	Dokumen Kerangka Kerja dari FIRST (FIRST, 2019a)
Deteksi dan Analisis	Berdasarkan artifak yang diberikan, terindikasi bahwa terdapat akses mencurigkan ke sebuah server yang termasuk dalam kategori IP dengan reputasi buruk, temukan IP tersebut?	File PCAP dari aktivitas mencurigkan
	Dari data log yang diberikan, terindikasi bahwa log tersebut menyerupai pola serangan dari salah satu *threat actor*, temukan teknik yang digunakan oleh *threat actor* tersebut?	Log serangan
	Dalam menjalankan tugas TTIS, TTIS harus memiliki mekanisme pelaporan, apakah mekanisme yang diwajibkan dan digunakan uji komunikasi oleh TTIS Sektoral?	Dokumen RFC-2350 dan Peraturan BSSN No 1 Tahun 2024 (BSSN, 2024)
Klasifikasi dan Prioritas	Dalam satu waktu, tim TTIS di organisasi mendapatkan laporan aduan terkait kebocoran data dari berbagai instansi, manakah yang di prioritaskan terlebih dahulu?	Laporan insiden dari berbagai konstituen TTIS
	Dari laporan yang diterima oleh TTIS, insiden kebocoran data termasuk berdampak pada aspek apa?	Laporan insiden siber dan Dokumen *Incident Response Plan* dari CMU bagian klasifikasi data (Carnegie Mellon University, 2014)
Respons Insiden	Berdasarkan kasus kebocoran data, data apa yang paling penting untuk ditinjau dalam analisis teknis oleh pihak ketiga untuk mengidentifikasi sumber dan dampak kebocoran?	Laporan Hasil Analisis Insiden
	Apa alasan utama perlunya personel penegak hukum dalam sebuah kasus insiden kebocoran data?	Standar Panduan Penanganan Insiden Siber dari NIST (Nelson et al., 2025)
	Apa langkah isolasi pertama yang diambil untuk menghentikan penyebaran insiden kebocoran data?	Buku Tim Penanganan Insiden Siber dan SANS (Patrick Kral, 2012)
	Berdasarkan panduan dari *Federal Trade Comission*, untuk mencegah semakin meluasnya kebocoran data. Apa yang harus dilakukan tim TTIS untuk mencegah hal tesebut	Panduan Respon Kebocoran Data dari Federal Trade Comission (Federal Trade Commission, 2021)
Pengumpulan Bukti dan Investigasi	Setelah diketahui perangkat yang terdampak, untuk mengambil alih barang bukti digital perlu untuk menggunakan metode forensik yang tepat,	Panduan Integrasi Teknik Forensik pada Respon Insiden dari NIST (Kent et al., 2006)

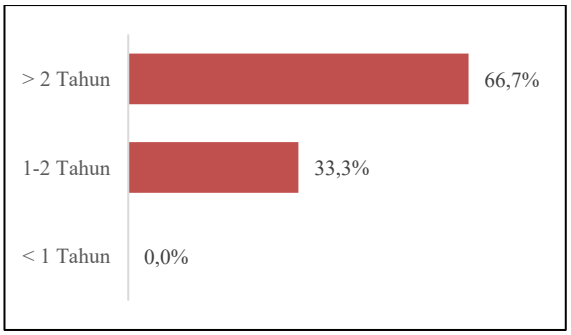
Tugas TTIS	Sampel Pertanyaan Evaluasi	Sampel Artifak
	disebut apa metode untuk mengambil data tersebut?	
	Berdasarkan hasil analisis, temukan akan permasalahan yang menyebabkan insiden tersebut bisa terjadi?	Pcap files dan log layanan
	Dalam melakukan analisis, tim TTIS dapat mengkorelasikan data dari berbagai macam sumber. Perangkat apa yang dapat dianalisis yang mencatat *security event information*?	Panduan Integrasi Teknik Forensik pada Respon Insiden dari NIST (Kent et al., 2006)
Eradikasi dan Pemulihan	Berdasarkan hasil analisis, temukan keseluruhan file yang dicurigai, sehingga dapat dilakukan penghapusan?	Log layanan
	Setelah pemulihan, bagaimana cara memastikan bahwa sistem yang sedang dipulihkan ke produksi tidak dikompromikan dengan metode yang sama yang menyebabkan insiden?	Standar Panduan Penanganan Insiden Siber dari NIST (Nelson et al., 2025)
Komunikasi dan Pelaporan	Berdasarkan insiden kebocoran data yang terjadi, dapatkan anda membuat rangkuman penanganan insiden yang bisa disampaikan ke media?	Standar Panduan Penanganan Insiden Siber dari NIST (Nelson et al., 2025)
	Berdasarkan bukti digital yang dikumpulkan, informasi apa yang paling relevan untuk disampaikan di persidangan dalam mendukung kasus kebocoran data?	Laporan Penanganan Insiden
	Apakah terdapat kewajiban untuk melaporan insiden beserta penanganannya TTIS Nasional atau Sektoral?	Peraturan BSSN No 1 Tahun 2024 (BSSN, 2024)
Evaluasi dan Pembelajaran	Apa langkah perbaikan spesifik yang direkomendasikan untuk mencegah kebocoran serupa di masa depan?	Laporan Penanganan Insiden
	Sebagai mekanisme pembelajaran untuk TTIS lainnya, informasi apa yang dapat dibagikan?	Dokumen Kerangka Kerja dari FIRST (FIRST, 2019a)

Pada Tabel 4 tersebut telah dijabarkan contoh pertanyaan teknis dan artefak yang relevan untuk setiap tugas dari TTIS. Pertanyaan tersebut disusun berdasarkan skenario kebocoran data yang mungkin terjadi. Sedangkan artifak akan digunakan sebagai data dukung personel yang dievaluasi untuk bisa menjawab pertanyaan yang diberikan. Selain itu kami juga membandingkan dengan beberapa kerangka terkait terhadap model yang telah kami susun. Pada Tabel 5 merupakan perbandingan dengan beberapa kerangka yang sudah ada. Selain itu, hasil perbandingan menunjukkan bahwa model kompetensi yang disusun memiliki keunggulan yaitu adanya tingkatan kompetensi, tahapan evaluasi lengkap, saran pengembangan kompetensi, serta fokus pada kesiapan operasional tim TTIS, yang menjadikannya unggul dibandingkan kerangka kerja yang sudah ada.

4.3. Validasi Model

Dari hasil validasi yang dilakukan melalui penyebaran kuesioner, model SCENE-CSIRT yang dikembangkan mendapat pengakuan yang baik dari para responden. Responden terdiri dari personel yang memiliki pengalaman langsung dalam pembentukan, evaluasi, dan pengembangan kompetensi TTIS. Pada Gambar 2 ditampilkan distribusi pengalaman responden, dimana sebagian besar memiliki pengalaman lebih dari dua tahun, yang menunjukkan bahwa responden tersebut memiliki dasar yang cukup dalam menilai model ini.

Gambar 3 menunjukkan distribusi pemahaman responden terkait tugas TTIS. Hasilnya memperlihatkan bahwa sebagian besar responden memiliki pemahaman yang baik terhadap berbagai aspek penting, seperti perencanaan dan persiapan, pengumpulan bukti dan investigasi, serta respon insiden.



Gambar 2. Distribusi Pengalaman Responden

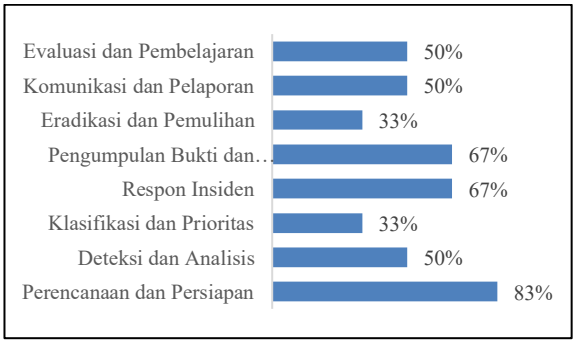
Pemahaman yang baik pada berbagai aspek ini menunjukkan bahwa responden memiliki pengetahuan yang memadai untuk memberikan penilaian yang valid terhadap model yang diuji. Pada tahap validasi model ini, penelitian telah menyusun pertanyaan yang diajukan validasi membagi dalam setiap tugas dari personel TTIS yang telah dipetakan. Setiap kategori tersebut terdiri dari aktivitas, aktivitas kompetensi, tingkatan kompetensi, rekomendasi peningkatan kompetensi, sampel pertanyaan evaluasi dan sampel artifak.

Tabel 5 Perbandingan terhadap instrumen lainnya

Perbandingan Penelitian	SIM 3 Versi 2 (Stikvoort, Kossakowski and Maj, 2023)	CREST *Cyber Security Incident Respons Maturity* (CREST, 2014)	Indeks KAMI V 5.0 (BSSN, 2023)	NIST CSF (NIST, 2024)	C2M2 (U.S Department of Energy, 2022)	Model Kompetensi yang disusun
Tujuan instrumen berkaitan dengan TTIS	Menilai kesiapan TTIS dalam merespons insiden	Menilai kemampuan tanggap insiden keamanan siber organisasi.	Menilai kesiapan sistem manajemen keamanan informasi untuk merespons insiden siber dan memastikan pemulihan serta keamanan informasi yang berkelanjutan	Menilai kemampuan organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari insiden siber dengan menggunakan kerangka kerja yang berbasis risiko	Menilai tingkat kematangan dan kesiapan organisasi dalam mengelola risiko dan insiden siber	Menilai kesiapan personel TTIS
Evaluasi Kompetensi Individu	-	-	-	-	✓	✓
Evaluasi Tingkatan Kompetensi Personel	-	-	-	-	-	✓
Tahapan Lengkap Penanganan Insiden	✓	✓	-	✓	✓	✓
Evaluasi Personel Berbasis *Evidence*	✓	✓	-	-	✓	✓
Saran Peningkatan Kompetensi	-	-	-	-	-	✓
Fokus Kesiapan Operasional Tim	✓	✓	-	✓	✓	✓

Berikut ini merupakan contoh penjabarannya.

a) Aktivitas: Membuat rencana tanggap insiden yang komprehensif.
b) Aktivitas Kompetensi: Mengembangkan dokumen rencana tanggap insiden sesuai dengan standar organisasi.
c) Tingkatan Kompetensi: Lanjutan.
d) Rekomendasi Peningkatan Kompetensi: LDR512: *Security Leadership Essentials for Managers - SANS* dan LDR514: *Security Strategic Planning, Policy, and Leadership – SANS*.
e) Sampel Pertanyaan Evaluasi:
Dalam dokumen *Incident Response Plan* (IRP) harus dijabarkan langkah yang harus diambil jika insiden kebocoran data yang terdeteksi tidak dapat ditangani oleh tim respons insiden organisasi?
f) Sampel Artifak : Dokumen *Incident Response Plan* dari CMU.



Gambar 3. Distribusi Pemahaman terkait Tugas TTIS dari Responden

Berdasarkan kategori tugas yang telah dijabarkan pada Tabel 6 merupakan rekapitulasi kesepakatan pakar dari hasil validasi model SCENE-CSIRT.

Tabel 6. Rekaptiulasi kesepakatan pakar

No	Aktivitas	Persentase Kesepakatan
1	Membuat rencana tanggap insiden yang komprehensif	100%
2	Melatih personel secara berkala dalam menghadapi insiden siber	100%
3	Memastikan setiap personel memahami perannya	100%
4	Mendeteksi adanya insiden	100%
5	Mengumpulkan informasi internal dan eksternal	83,3%
6	Menerima dan menindaklanjuti laporan insiden dari konstituen	100%
7	Menentukan tingkat urgensi insiden	100%
8	Menilai dampak insiden	100%
9	Melakukan isolasi untuk meminimalkan kerugian lebih lanjut	100%
10	Melakukan mitigasi sesuai rencana tanggap insiden	100%
11	Menerapkan pertahanan untuk mencegah penyebaran insiden	83,3%
12	Mengumpulkan bukti digital dari berbagai sumber	83,3
13	Menganalisis bukti untuk memahami akar masalah	100%
14	Menganalisis log file dan mengkorelasikan insiden terkait	100%
15	Menghilangkan file mencurigakan yang terkait ancaman	100%
16	Memulihkan sistem ke kondisi normal setelah ancaman dihapus	100%
17	Memberikan informasi ke media, penegak hukum, dan pihak terkait lainnya	100%
18	Melaporkan insiden ke TTIS Sektor atau TTIS Nasional sesuai regulasi	100%
19	Meninjau efektivitas respons yang telah dilakukan	100%
20	Membagikan informasi insiden dan detail penanganan dengan konstituen dan TTIS lainnya	100%
21	Membuat rencana tanggap insiden yang komprehensif	100%
22	Melatih personel secara berkala dalam menghadapi insiden siber	100%
Presentase Kesepakatan Total		**97.72%**

Secara keseluruhan seperti yang dapat dilihat pada Tabel 6 bahwa tanggapan responden menunjukkan bahwa model evaluasi ini relevan dan mencakup aspek-aspek yang dibutuhkan oleh personel TTIS dalam menangani insiden siber. Berdasarkan hasil ini, model evaluasi dianggap valid untuk mengukur keterampilan TTIS serta memberikan umpan balik yang efektif dalam perbaikan keterampilan. Selain itu, model ini dinilai dapat berfungsi sebagai alat yang berguna dalam meningkatkan kualitas penanganan insiden siber di lingkungan pemerintahan.

Selain itu, terdapat beberapa masukan terkait dengan pertanyaan yang digunakan dalam mengevaluasi kemampuan personel. Oleh karena itu, agar pengukuran kemampuan personel TTIS menggunakan model ini lebih efektif dan akurat, disarankan untuk melengkapinya dengan studi kasus langsung yang relevan dengan sektor yang bersangkutan. Melalui penerapan studi kasus nyata, personel dapat dihadapkan pada situasi insiden siber yang serupa dengan kondisi nyata yang mungkin mereka hadapi. Hal ini memungkinkan pengujian keterampilan teknis dan non-teknis secara lebih komprehensif serta memastikan bahwa model evaluasi tidak hanya teoritis, tetapi juga aplikatif dalam konteks operasional sektor terkait. Studi kasus langsung juga akan memberikan gambaran yang lebih jelas mengenai kekuatan dan kelemahan personel, sehingga hasil evaluasi dapat digunakan secara efektif untuk meningkatkan kompetensi dan kesiapan TTIS dalam penanganan insiden di sektor tersebut.

5. KESIMPULAN

Pada penelitian ini kami, telah mengembangkan dan menguji model SCENE-CSIRT yang dirancang khusus untuk personel TTIS di lingkungan pemerintah daerah. Model ini mengadopsi pendekatan berbasis skenario yang terbukti efektif dalam menilai keterampilan yang sangat penting bagi personel TTIS. Hasil penelitian ini menunjukkan bahwa model tersebut mampu mengidentifikasi kesenjangan keterampilan yang ada, sekaligus menyediakan kerangka kerja untuk pengembangan program peningkatan kompetensi yang lebih terarah dan berkelanjutan.

Penelitian ini diharapkan dapat menjadi acuan bagi pengembangan kebijakan terkait pembentukan dan peningkatan kapasitas TTIS di lingkungan pemerintah daerah, sehingga TTIS dapat menjadi lebih tangguh dan responsif dalam menghadapi ancaman serta insiden siber yang semakin kompleks. Selain itu, model evaluasi ini memberikan dasar yang bagi pengukuran keterampilan TTIS secara menyeluruh dan mendukung peningkatan kualitas penanganan insiden di pemerintah daerah. Sebagai langkah selanjutnya, disarankan untuk menerapkan model ini melalui studi kasus di instansi terkait guna memperoleh bukti nyata bahwa model ini dapat berfungsi secara efektif sebagai alat evaluasi kompetensi TTIS dalam situasi nyata.

DAFTAR PUSTAKA

ALBERTS, C., DOROFEE, A., KILLCRECE, G., RUEFLE, R. and ZAJICEK, M., 2004a. *Defining Incident Management Processes for CSIRTs: A Work in Progress*.

ALBERTS, C., DOROFEE, A., KILLCRECE, G., RUEFLE, R. and ZAJICEK, M., 2004b. *Defining Incident Management Processes for CSIRTs: A Work in Progress*.

ALOTHMAN, B., ALHAJRAF, A., ALAJMI, R., AL FARRAJ, R., ALSHAREEF, N. and KHAN, M., 2022. Developing a Cyber Incident Exercises Model to Educate Security Teams. *Electronics 2022, Vol. 11, Page 1575*, [online] 11(10), p.1575. https://doi.org/10.3390/ELECTRONICS11101575.

ANGAFOR, G.N., YEVSEYEVA, I. and MAGLARAS, L., 2023. Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information and Computer Security*, 31(4), pp.404–426. https://doi.org/10.1108/ICS-05-2022-0085/FULL/PDF.

BSSN, 2019. *Peta Okupasi Nasional dalam Kerangka Kualifikasi Nasional Indonesia pada Area Fungsi Keamanan Siber*.

BSSN, 2023. *Indeks KAMI Versi 5.0*. [online] Available at: <https://www.bssn.go.id/indeks-kami/> [Accessed 27 April 2025].

BSSN, 2024. Peraturan BSSN No. 1 Tahun 2024.

BSSN, 2025. Lanskap Keamanan Siber Indonesia 2024. pp.1–107.

Carnegie Mellon University, 2014. *Computer Security Incident Response Plan*.

CREST, 2014. Introduction Cyber Security Incident response process.

Federal Trade Commission, 2021. *Data Breach Response: A Guide for Business | Federal Trade Commission*. [online] Available at: <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> [Accessed 4 November 2024].

FIRST, 2019a. CSIRT Roles and Competences (Addendum).

FIRST, 2019b. *CSIRT Services Framework Version 2.1*. [online] Available at: <https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1> [Accessed 8 October 2024].

FORTINET, 2024. *2024 Cybersecurity Skills Gap Global Research Report*.

FURNELL, S., 2021. The cybersecurity workforce and skills. *Computers & Security*, 100, p.102080. https://doi.org/10.1016/J.COSE.2020.102080.

GEBREMESKEL, B.K., JONATHAN, G.M. and YALEW, S.D., 2023. Information Security Challenges During Digital Transformation. *Procedia Computer Science*, 219, pp.44–51. https://doi.org/10.1016/J.PROCS.2023.01.262.

GFCE, 2019. Global CSIRT Maturity Framework Stimulating the development and maturity enhancement of national CSIRTs.

GHOSH, T. and FRANCIA, G., 2021. Assessing Competencies Using Scenario-Based Learning in Cybersecurity. *Journal of Cybersecurity and Privacy 2021, Vol. 1, Pages 539-552*, [online] 1(4), pp.539–552. https://doi.org/10.3390/JCP1040027.

HRANICKÝ, R., BREITINGER, F., RYŠAVÝ, O., SHEPPARD, J., SCHAEDLER, F., MORGENSTERN, H. and MALIK, S., 2021. What do incident response practitioners need to know? A skillmap for the years ahead. *Forensic Science International: Digital Investigation*, 37, p.301184. https://doi.org/10.1016/J.FSIDI.2021.301184.

JASON KICK, 2014. *Cyber Exercise Playbook*.

KENT, K., CHEVALIER, S., GRANCE, T. and DANG, H., 2006. Guide to Integrating Forensic Techniques into Incident Response. [online] https://doi.org/10.6028/NIST.SP.800-86.

KOUTSOURIS, N., VASSILAKIS, C. and KOLOKOTRONIS, N., 2021. Cyber-security training evaluation metrics. *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, pp.192–197. https://doi.org/10.1109/CSR51186.2021.9527946.

MARTIN, A., SCHNEIDER, S., RIGBY, Y. and HALLETT, J., 2021. *The Cyber Security Body of Knowledge*. The National Cyber Security Centre 2021.

NELSON, A., REKHI, S., SOUPPAYA, M. and SCARFONE, K., 2025. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. https://doi.org/10.6028/NIST.SP.800-61R3.

NIST, 2024. The NIST Cybersecurity Framework (CSF) 2.0. [online] https://doi.org/10.6028/NIST.CSWP.29.

NORRIS, D., JOSHI, A. and FININ, T., 2015. Cybersecurity Challenges to American State and Local Governments. *15th European Conference on eGovernment*, pp.196–202.

Northern Illinois University Center for Innovative Teaching and Learning, 2012. *Rubrics for assessment.* [online] Available at: <https://www.niu.edu/citl/resources/guides/instructional-guide>.

PATRICK KRAL, 2012. *Incident Handler's Handbook*.

PETERSEN, R., SANTOS, D., SMITH, M.C., WETZEL, K.A. and WITTE, G., 2020a. Workforce Framework for Cybersecurity (NICE Framework). [online] https://doi.org/10.6028/NIST.SP.800-181R1.

PETERSEN, R., SANTOS, D., SMITH, M.C., WETZEL, K.A. and WITTE, G., 2020b. Workforce Framework for Cybersecurity (NICE Framework). [online] https://doi.org/10.6028/NIST.SP.800-181R1.

PRABASWARI, P., ALFIKRI, M. and AHMAD, I., 2022. Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan*, 6(1), pp.1–14. https://doi.org/10.21787/mp.6.1.2022.1-14.

Presiden Republik Indonesia, 2019. *Peraturan Presiden Republik Indonesia Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024*.

SALWA, N.D.K., 2024. *Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia*.

[online] Available at: <https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn> [Accessed 26 January 2025].

Software Engineering Institute, 2017. *What Skills are Needed when Staffing your CSIRT?*

STIKVOORT, D., KOSSAKOWSKI, K.-P. and MAJ, M., 2023. SIM3 v2 interim-Security Incident Management Maturity Model Acknowledgement and Justification.

U.S Department of Energy, 2022. *Cybersecurity Capability Maturity Model (C2M2)*.

VILLEGAS-CH, W., ORTIZ-GARCES, I. and SÁNCHEZ-VITERI, S., 2021. Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *Computers 2021, Vol. 10, Page 102*, [online] 10(8), p.102. https://doi.org/10.3390/COMPUTERS10080102.