Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 5, Mei 2025, Hal. 1265-1279
DOI: https://doi.org/10.52436/1.jpti.715
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Pengembangan Skenario Serangan Siber untuk Pelatihan Tim Tanggap Insiden Siber Pemerintah Daerah Menggunakan *Framework* MITRE ATT&CK dan *Cyber Kill Chain*

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

[1,2]Teknik Elektro, Universitas Indonesia, Indonesia
Email: [1]faizal.wahyu@ui.ac.id, [2]muhammad.salman@ui.ac.id

Abstrak

Keamanan siber menjadi tantangan utama bagi organisasi dalam menghadapi ancaman seperti *phishing*, *malware*, dan eksploitasi kerentanan. Penelitian ini mengembangkan dan memvalidasi skenario serangan siber untuk meningkatkan kesiapan Tim Tanggap Insiden Siber (TTIS) di pemerintah daerah. Skenario yang dikembangkan mencakup pencurian kredensial melalui *phishing* dan *malware stealer*, serta eksploitasi kerentanan aplikasi *web* untuk menyisipkan situs judi *online* ilegal. Penyusunan skenario menggunakan *framework* MITRE ATT&CK dan metodologi *Cyber Kill Chain* guna memetakan teknik serangan secara sistematis. Validasi dilakukan melalui *expert judgement* oleh pakar keamanan siber untuk menilai realisme dan relevansi skenario terhadap ancaman nyata. Hasil validasi menunjukkan bahwa skenario ini sesuai dengan ancaman terkini dan mencerminkan celah keamanan yang sering dimanfaatkan oleh penyerang. Evaluasi skenario menunjukkan bahwa latihan berbasis serangan nyata meningkatkan deteksi insiden serta efektivitas respons tim. Penelitian ini berkontribusi dalam penyempurnaan metode pelatihan keamanan siber di sektor publik dengan menyediakan skenario berbasis ancaman yang kontekstual. Hasil penelitian dapat digunakan untuk meningkatkan strategi pelatihan dan optimalisasi alat pendukung. Penelitian selanjutnya dapat mengembangkan skenario serangan tambahan, seperti ransomware dan *Advanced Persistent Threats* (APT), serta mengintegrasikan teknik deteksi otomatis guna meningkatkan kesiapan TTIS.

Kata kunci: *Malware Stealer, Pencurian Kredensial, Pelatihan Keamanan Siber, Phishing, Skenario Serangan Siber, Tim Tanggap Insiden Siber (TTIS).*

Development of Cyber Attack Scenarios for Incident Response Team Training in Local Government Using the MITRE ATT&CK and Cyber Kill Chain Frameworks

Abstract

Cybersecurity is a major challenge for organizations in addressing threats such as phishing, malware, and vulnerability exploitation. This study develops, validates, and tests cyber-attack scenarios to enhance the readiness of the Cyber Security Incident Response Team (CSIRT) in local government. The scenarios include credential theft through phishing and stealer malware, as well as the exploitation of web application vulnerabilities to inject illegal gambling sites. The scenario development follows the MITRE ATT&CK framework and Cyber Kill Chain methodology to systematically map attack techniques. Validation was conducted through expert judgment by cybersecurity professionals to assess the realism and relevance of the scenarios to real-world threats. The validation results indicate that the scenarios align with current threats and reflect security gaps frequently exploited by attackers. Scenario evaluation demonstrates that real-world attack-based training improves incident detection and response effectiveness. This study contributes to improving cybersecurity training methods in the public sector by providing threat-based, contextual scenarios. The findings can be used to refine training strategies and optimize supporting tools. Future research may expand attack scenarios, such as ransomware and Advanced Persistent Threats (APT), and integrate automated detection techniques to enhance CSIRT preparedness.

Keywords: *Computer Security Incident Response Team (CSIRT), Credential Theft, Cyber Attack Scenario, Cybersecurity Training, Malware Stealer, Phishing.*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

1. PENDAHULUAN

Dalam era digital yang berkembang pesat, pemerintah daerah di Indonesia semakin bergantung pada sistem informasi dan teknologi untuk meningkatkan kualitas pelayanan publik. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) mendorong adopsi teknologi untuk meningkatkan efisiensi dan efektivitas layanan [1], [2]. Namun, peningkatan ketergantungan ini juga diiringi dengan meningkatnya ancaman siber yang semakin kompleks. Insiden siber tidak hanya berpotensi mengganggu pelayanan publik tetapi juga dapat menyebabkan kerugian finansial serta merusak reputasi pemerintah daerah [3]. Oleh karena itu, kesiapan dalam menghadapi ancaman siber menjadi hal yang sangat penting, salah satunya melalui latihan keamanan siber secara berkala.

Saat ini, banyak pemerintah daerah telah membentuk Tim Tanggap Insiden Siber (TTIS) yang bertugas mendeteksi dan merespons ancaman siber secara cepat dan efisien [4]. TTIS memiliki peran krusial dalam mengidentifikasi serangan, merespons insiden, serta menerapkan mitigasi untuk mengurangi dampak yang ditimbulkan [5]. Namun, penelitian menunjukkan bahwa banyak TTIS masih memiliki keterbatasan dalam kesiapan teknis dan koordinasi saat menangani insiden siber seperto terkendala terkait dengan kurangnya sumber daya manusia dengan kompetensi yang memadai [6], [7], [8].

Untuk mengatasi keterbatasan ini, latihan keamanan siber berbasis skenario menjadi pendekatan yang efektif. Latihan ini dirancang untuk memperkuat kemampuan teknis dan koordinasi TTIS dalam menghadapi serangan siber secara lebih terstruktur dan realistis [9], [10]. Dengan melibatkan skenario-skenario yang realistis, pelatihan dapat membantu tim meningkatkan keterampilan dalam mendeteksi, merespons, dan memitigasi serangan siber [11]. Latihan tersebut juga mempersiapkan tim dalam menghadapi situasi yang mungkin tidak terduga, sehingga mereka lebih siap untuk menghadapi ancaman yang terus berkembang. Simulasi berbasis mesin virtual juga terbukti lebih efisien dibandingkan metode konvensional, karena memungkinkan peserta untuk berlatih dalam lingkungan yang aman tanpa memerlukan infrastruktur fisik yang kompleks [12]. Dengan skenario latihan yang realistis, tim dapat meningkatkan keterampilan dalam mendeteksi, merespons, dan memitigasi serangan siber secara optimal.

Selain meningkatkan keterampilan teknis, latihan keamanan siber yang terstruktur juga berkontribusi pada peningkatan kesadaran terhadap ancaman siber dan efektivitas rencana respons insiden [13]. Latihan yang berkelanjutan dapat membantu dalam pengujian dan pembaruan kebijakan keamanan, serta meningkatkan kesiapan organisasi dalam menghadapi insiden siber yang semakin kompleks[14].

Penelitian ini bertujuan untuk mengembangkan skenario latihan keamanan siber yang relevan dan aplikatif bagi pemerintah daerah di Indonesia. Dengan pendekatan berbasis skenario, penelitian ini diharapkan dapat membantu meningkatkan kesiapan TTIS dalam menghadapi ancaman siber melalui latihan yang realistis dan sistematis. Metode penelitian mencakup studi literatur, analisis kebutuhan, perancangan skenario, serta validasi melalui uji coba pelatihan guna memastikan efektivitasnya dalam meningkatkan kompetensi teknis dan respons tim terhadap insiden siber.

2. PENELITIAN TERKAIT

Dalam era transformasi digital, keamanan siber telah menjadi salah satu elemen paling kritis bagi organisasi untuk melindungi data, sistem, dan infrastruktur penting. Untuk memastikan kesiapan dalam menghadapi insiden siber, penyusunan skenario pelatihan yang terstruktur dan mendalam menjadi sangat penting, khususnya bagi Tim Tanggap Insiden Siber (TTIS**)**. Skenario pelatihan yang realistis memungkinkan TTIS untuk menghadapi simulasi serangan siber yang mencerminkan ancaman nyata. Dengan adanya pelatihan berbasis ancaman aktual, banyak manfaat yang dapat diperoleh, seperti meningkatkan ketepatan deteksi dan respons teknis terhadap serangan yang semakin kompleks. Hal ini juga mempermudah pengujian prosedur tanggap insiden serta membantu mengidentifikasi celah keamanan dalam proses internal organisasi, yang dapat berkontribusi pada kesiapan tim dalam mengatasi insiden yang terjadi [15]

Skenario pelatihan berbasis ancaman aktual memiliki peran kunci dalam memperkuat ketahanan dan respons tim TTIS. Menurut salah satu artikel, dalam menyusun pelatihan keamanan siber, sering kali digunakan jenis *table-top exercise* (TTX) [16]. TTX ini umumnya difokuskan pada simulasi yang berbasis diskusi, di mana berbagai peran dan tanggung jawab dalam organisasi dilibatkan. Namun, pendekatan ini lebih mengutamakan simulasi berbasis keputusan strategis yang relevan dengan anggota organisasi non-teknis, bukan dengan anggota TTIS yang berfokus pada aspek teknis. Skenario yang ideal bagi TTIS hendaknya melibatkan latihan yang lebih bersifat praktis dan langsung, seperti analisis forensik digital, analisis log, serta mitigasi ancaman secara langsung dengan memanfaatkan alat-alat yang umum digunakan dalam tim tanggap insiden [17].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

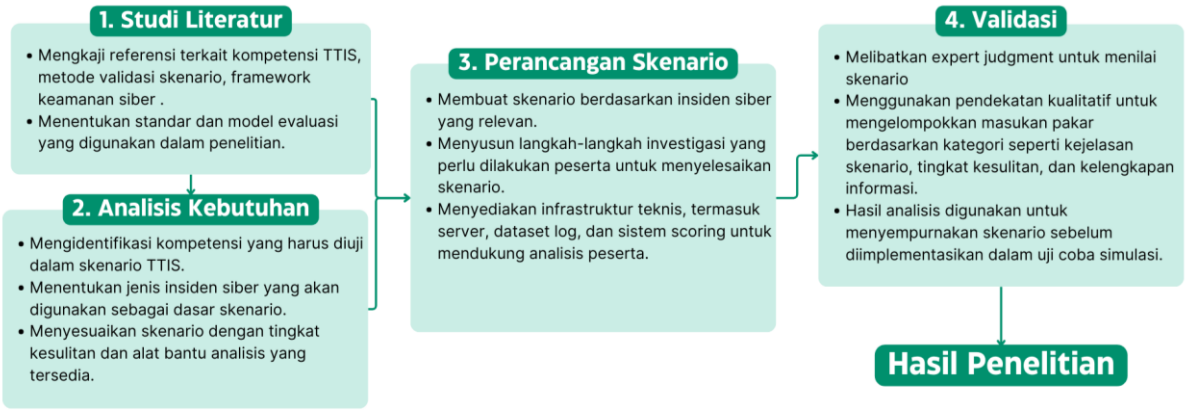
Beberapa penelitian juga membahas penggunaan skenario berbasis ancaman untuk mengatasi hambatan sosial-teknis dalam koordinasi tim respons insiden [18]. Penelitian ini memberikan wawasan mengenai pentingnya aspek sosial dalam respon terhadap ancaman. Namun, dalam hal ini, penerapan teknis terkait simulasi yang melibatkan infrastruktur TI secara langsung, seperti penggunaan server virtualisasi atau lingkungan khusus yang menyediakan pengalaman lapangan dalam menghadapi ancaman nyata, belum cukup ditekankan. Untuk itu, penelitian lebih lanjut dibutuhkan untuk mengembangkan skenario pelatihan yang lebih realistis bagi tim TTIS dengan memperhitungkan kebutuhan praktis akan alat dan teknologi yang ada.

Meskipun beberapa penelitian telah menekankan pada pelatihan berbasis skenario dan pentingnya pengelolaan insiden secara komprehensif, evaluasi yang lebih rinci mengenai efektivitas dari skenario tersebut dalam melatih tim TTIS terhadap ancaman yang lebih baru dan kompleks masih sangat terbatas. Pengembangan lebih lanjut mengenai evaluasi teknis dan metode pelatihan berbasis simulasi langsung perlu menjadi prioritas agar tim TTIS benar-benar siap menangani ancaman yang semakin kompleks dan dinamis dalam dunia maya [5].

Dalam upaya meningkatkan kesiapan tim TTIS, beberapa pihak telah mengimplementasikan solusi pelatihan berbasis simulasi yang mendalam atau yang lebih dikenal dengan *Cyber Range*. Dengan adanya *platform* tersebut dapat menciptakan simulasi realistis untuk memandu tim melalui skenario pelanggaran siber tingkat perusahaan. Penelitian terkait juga telah mengembangkan *platform* yang dapat digunakan untuk melakukan simulasi [19], [20], [21], [22], [23], [24]. Dengan demikian, pengembangan skenario pelatihan yang lebih realistis dan teknis, serta evaluasi yang lebih mendalam mengenai efektivitasnya, menjadi langkah penting dalam meningkatkan kesiapan tim TTIS dalam menghadapi ancaman siber yang semakin kompleks yang juga dapat di integrasikan ke *platform* terkait.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan tujuan untuk menyusun skenario latihan keamanan siber yang relevan dan aplikatif bagi pemerintah daerah di Indonesia. Metodologi ini dirancang untuk mengidentifikasi kebutuhan, memahami karakteristik ancaman yang dihadapi, dan menghasilkan desain skenario yang sesuai dengan konteks lokal pemerintah daerah. Langkah-langkah yang diterapkan dalam penelitian ini dijelaskan secara rinci pada Gambar 1 berikut.



Gambar 1. Alur Penelitian

3.1. Studi Literatur

Pada tahap studi literatur, peneliti mengumpulkan berbagai data sekunder yang berasal dari jurnal internasional, laporan keamanan siber nasional seperti yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN) serta Tim Tanggap Insiden Siber (TTIS) di Indonesia, dan juga laporan dari lembaga internasional seperti *National Institute of Standards and Technology* (NIST) [25], *Department of Home Affairs Australian Government* [26] dan *European Network and Information Security Agency* (ENISA) [27]. Pengumpulan data ini bertujuan untuk menggali informasi mendalam mengenai beberapa aspek penting dalam penyusunan skenario latihan keamanan siber.

Peneliti pertama-tama fokus pada identifikasi jenis ancaman siber yang sering kali dihadapi oleh sektor pemerintahan, baik itu ancaman dari luar maupun yang bersifat internal. Menurut laporan BSSN, sektor

p-ISSN: 2775-4227
e-ISSN: 2775-4219

pemerintah adalah target utama dari serangan siber dengan pola serangan yang terus berkembang [3]. Laporan tersebut juga mengungkapkan bahwa sektor publik menghadapi ancaman yang bervariasi.

3.2. Analisis Kebutuhan

Analisis kebutuhan dalam penelitian ini dilakukan dengan mengumpulkan data primer melalui wawancara mendalam yang ditujukan kepada unit kerja terkait di Badan Siber dan Sandi Negara (BSSN) yang bertanggung jawab atas pembinaan keamanan siber di pemerintah daerah. Proses wawancara bertujuan untuk memahami kebutuhan, tantangan, dan perspektif dalam melaksanakan program pembinaan keamanan siber secara efektif.

Data yang diperoleh dari wawancara dianalisis untuk mengidentifikasi pola, kesenjangan, serta kebutuhan spesifik terkait peningkatan kapasitas keamanan siber di pemerintah daerah. Untuk memperkuat hasil wawancara, penelitian ini juga menggunakan studi literatur sebagai metode pelengkap dengan menelaah dokumen resmi, kebijakan keamanan siber nasional, serta kerangka kerja internasional yang relevan. Hasil dari kedua metode tersebut menjadi dasar dalam perumusan rekomendasi program pembinaan keamanan siber yang sesuai dengan kondisi pemerintah daerah.

3.3. Perancangan Skenario Latihan

Skenario latihan disusun berdasarkan hasil studi literatur yang mendalam dan analisis kebutuhan yang telah dilakukan sebelumnya. Proses perancangan skenario ini bertujuan untuk menghasilkan latihan yang relevan dan efektif bagi pemerintah daerah dalam menghadapi ancaman siber yang ada. Berikut ini meruapakan tahapan dalam dalam perancangan skenario latihan yang terdiri dari:

1. Penentuan Tujuan Latihan

Pada tahapan awal dalam perancangan skenario yaitu penentuan tujuan dari latihan yang akan dilaksanakan. Tujuan skenario latihan ditentukan berdasarkan kebutuhan yang diidentifikasi melalui wawancara dan studi literatur. Tujuan ini bisa beragam, seperti meningkatkan kemampuan deteksi dini terhadap ancaman, mempercepat respons insiden, atau mengoptimalkan langkah-langkah mitigasi terhadap kerentanan yang ada.

2. Identifikasi Ancaman Siber Relevan

Ancaman siber yang dipilih untuk dimasukkan ke dalam skenario latihan didasarkan pada jenis serangan yang paling sering dihadapi oleh pemerintah daerah. Ancaman-ancaman ini diidentifikasi dengan mengacu pada data yang diperoleh dari laporan BSSN, wawancara dengan unit kerja terkait, serta literatur yang ada. Jenis serangan yang relevan termasuk *ransomware*, *phishing*, serangan DDoS (*Distributed Denial of Service*), insiden terkait kebocoran data serta insiden yang terkait dengan pemerintah daerah. Fokus pada ancaman yang paling sering terjadi ini akan memastikan bahwa latihan yang dirancang mencerminkan kenyataan dan menghadirkan pengalaman yang relevan bagi peserta.

3. Perancangan Alur Skenario

Setelah tujuan dan ancaman yang relevan ditetapkan, skenario latihan dirancang dengan memperhatikan tiga tahap utama. Penyusunan skenario ini melibatkan beberapa langkah, antara lain:

a. Identifikasi Ancaman dan Teknik Serangan

Tahap awal melibatkan pemodelan serangan yang menargetkan infrastruktur organisasi. Teknik serangan dipilih berdasarkan hasil studi literatur dan wawancara dengan pihak terkait, lalu dipetakan menggunakan *framework* MITRE ATT&CK [28]. Framework ini digunakan untuk mengklasifikasikan ancaman secara terstruktur, sehingga setiap teknik serangan dapat dimengerti dalam konteks nyata dan dikaitkan dengan tindakan mitigasi yang relevan.

b. Penyusunan Langkah-Langkah Serangan

Tahap ini bertujuan untuk merancang rangkaian serangan secara sistematis, mencakup berbagai metode yang sering digunakan oleh penyerang. Fokusnya adalah menggambarkan interaksi antara penyerang dan sistem, termasuk skenario umum seperti serangan berbasis aplikasi web atau eksploitasi sistem.

c. Pemetaan ke *Cyber Kill Chain*

Setelah langkah-langkah serangan tersusun, tahapan ini dipetakan ke model *Cyber Kill Chain* [29]. Framework ini digunakan untuk menggambarkan bagaimana serangan berlangsung secara berurutan, dari *Reconnaissance*, *Weaponization*, hingga *Actions on Objectives*. Tujuannya adalah memberikan pemahaman yang menyeluruh tentang setiap tahap serangan, sehingga memungkinkan tim untuk mengidentifikasi celah keamanan dan strategi pertahanan yang tepat di setiap langkah.

d. Penyesuaian Konteks di Indonesia

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Skenario latihan yang sudah dirancang selanjutnya disesuaikan dengan kondisi di Indonesia, seperti infrastruktur teknologi yang tersedia di pemerintah daerah dan kompetensi SDM yang terlibat. Contohnya, jika terdapat keterbatasan perangkat keras atau perangkat lunak, skenario akan dirancang agar tetap relevan dan efektif dalam batasan yang ada. Penyesuaian juga mencakup tingkat pengalaman peserta, sehingga skenario cocok untuk berbagai level kompetensi, mulai dari pemula hingga profesional tingkat lanjut.

3.4. Validasi Skenario

Dalam penelitian ini, validasi skenario dilakukan menggunakan metode *expert judgment*, di mana para pakar di bidang keamanan siber menilai kelayakan dan kualitas skenario yang dirancang. Validasi ini bertujuan untuk memastikan bahwa skenario sesuai dengan tantangan dunia nyata serta efektif dalam meningkatkan kompetensi peserta.

1. Pemilihan Pakar

Pakar yang terlibat dalam validasi skenario dipilih berdasarkan kriteria berikut:

- Memiliki pengalaman kerja di bidang keamanan siber, khususnya dalam *incident response* atau *digital forensics* (minimal 5 tahun).
- Pernah terlibat dalam pengembangan, pelatihan, simulasi, atau evaluasi kompetensi keamanan siber.

Untuk memastikan keberagaman perspektif, penelitian ini melibatkan minimal 3–5 pakar dari berbagai latar belakang, seperti praktisi industri, akademisi, dan anggota TTIS yang aktif menangani insiden.

2. Validasi oleh Pakar

Pakar yang terlibat akan mengevaluasi skenario berdasarkan empat elemen utama:

- Relevansi dengan insiden dunia nyata → Apakah skenario mencerminkan ancaman dan serangan yang sering terjadi dalam lingkungan operasional?
- Kejelasan dan kelengkapan informasi → Apakah skenario menyediakan cukup data bagi peserta untuk menganalisis insiden tanpa ambiguitas?
- Kompleksitas sesuai tingkat kompetensi peserta → Apakah tingkat kesulitan skenario sesuai dengan tingkat keahlian yang ingin diuji?
- Keberadaan elemen pendukung → Apakah infrastruktur (server, aplikasi, dan alat analisis) sudah cukup mendukung proses investigasi yang dilakukan peserta?

3. Proses Penilaian dengan Kuisioner

Pakar akan diberikan dokumen skenario beserta lembar kuisioner untuk memberikan penilaian terhadap setiap aspek skenario. Skala penilaian menggunakan tiga kategori:

- Setuju → Skenario sudah sesuai dan tidak memerlukan perbaikan.
- Setuju dengan masukan → Skenario sudah cukup baik tetapi perlu perbaikan atau penyesuaian tertentu.
- Tidak setuju → Skenario tidak sesuai dan memerlukan revisi signifikan.

Jika pakar memilih "Setuju dengan masukan" atau "Tidak setuju," mereka harus memberikan alasan dan saran perbaikan. Data dari kuisioner akan dianalisis untuk mengidentifikasi aspek skenario yang perlu disempurnakan sebelum diterapkan dalam uji coba simulasi.

4. Pengolahan Data

Pengolahan data dalam penelitian ini dilakukan secara sistematis untuk memastikan bahwa masukan dari pakar dapat diinterpretasikan dengan baik dan digunakan untuk memperbaiki skenario evaluasi kompetensi TTIS. Tahapan pertama adalah pengumpulan data, yang diperoleh melalui kuisioner. Kuisioner ini terdiri dari tiga pilihan, yaitu setuju, setuju dengan masukan, dan tidak setuju. Jika pakar memberikan masukan atau tidak setuju, mereka diwajibkan memberikan alasan dan rekomendasi perbaikan. Selain kuisioner, wawancara tambahan dengan pakar juga dapat dilakukan untuk mendapatkan pemahaman yang lebih mendalam terkait masukan yang diberikan.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Studi Literatur

Penelitian ini memanfaatkan studi literatur untuk memetakan berbagai tantangan dalam keamanan siber pemerintah daerah. Dari berbagai literatur internasional dan laporan nasional, diperoleh beberapa temuan, antara lain:

1. Ancaman Siber Utama

- *Phishing* menjadi ancaman serius karena kurangnya kesadaran pengguna dan kurang efektifnya pengelolaan email. Hal tersebut juga diperkuat dengan laporan dari BSSN yang menyatakan bahwa terdapat

p-ISSN: 2775-4227
e-ISSN: 2775-4219

indikasi *phising* di Indonesia pada tahun 2024 sekitar 26 juta aktivitas [3]. Diperlukan program edukasi kepada pegawai pemerintah daerah tentang cara mengenali upaya *phishing*, implementasi email filtering untuk mendeteksi aktivitas mencurigakan, serta penerapan otentikasi multifaktor untuk mengamankan akses ke sistem penting.

- *Stealer Malware* menjadi ancaman yang serius selama periode tahun 2024 [30]. Malware jenis ini dirancang secara khusus untuk mencuri informasi dari target korban, seperti kredensial login, informasi perbankan, dan data sensitif lainnya. Serangan *Stealer Malware* biasanya dilakukan melalui berbagai teknik, termasuk distribusi melalui *email phishing*, *exploit kits*, atau penyebaran di situs web berbahaya.

4.2. Analisis Kebutuhan

Hasil analisis kebutuhan dilakukan melalui wawancara dengan pihak terkait. Hasilnya mengungkapkan tantangan utama yang dihadapi oleh pemerintah daerah, yaitu:

1. Skenario Insiden

Saat ini *server* pemerintah daerah sering menjadi target eksploitasi oleh pelaku judi *online* melalui serangan web atau penyalahgunaan infrastruktur jaringan [3], [31]. Hal tersebut juga didukung dengan fokus dari pemerintah dalam memberantas judi *online*. Sehingga pada skenario yang disusun berfokus pada insiden yang saat ini terjadi yaitu eksploitasi judi *online* pada situs *website*.

2. Identifikasi Infrastruktur

Berdasarkan penelitian Yudhanti dan Safitri [32], menunjukkan bahwa penggunaan *Security Information and Event Management* (SIEM) Elastic mempunyai keunggulan dalam mendeteksi ancaman kejahatan siber pada sistem jaringan layanan e-*Government* dengan cepat dan akurat. Berdasarkan hal tersebut, pada skenario yang akan disusun akan menggunakan SIEM tersebut yang akan digunakan oleh personel TTIS untuk melakukan analisis log terhadap insiden yang terjadi.

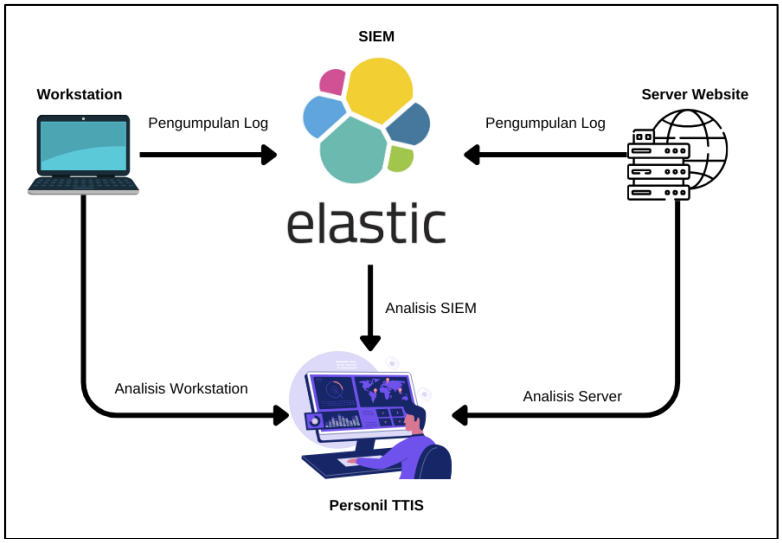
4.3. Penyusunan Skenario Latihan

Hasil dari studi literatur dan analisis kebutuhan digunakan untuk merancang skenario latihan yang memenuhi kebutuhan pemerintah daerah. Pendekatan yang diambil adalah mengembangkan skenario dengan kerangka sebagai berikut:

1. Tujuan Skenario

Tujuan dari skenario latihan ini adalah untuk melatih kemampuan personel TTIS di pemerintah daerah, terutama dalam menangani setiap tahapan proses penanganan insiden [25]. Skenario yang dikembangkan dirancang untuk memberikan pemahaman praktis dan keterampilan yang diperlukan dalam mendeteksi, merespons, dan memitigasi ancaman siber secara efektif. Dengan berfokus pada tahapan-tahapan kritis, mulai dari identifikasi awal hingga pemulihan setelah insiden, pelatihan ini bertujuan untuk meningkatkan ketangkasan dan koordinasi tim TTIS dalam mengatasi insiden siber dengan cara yang terstruktur dan efisien.

2. Tahapan Skenario



Gambar 1. Alur Skenario

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Berikut penjelasan alur pada Gambar 1 yang melibatkan *Workstation*, SIEM, *server* target, dan personel SOC:

- Pemantauan dan pengumpulan *log* dari komputer dan server target

Komputer dan *server* target yang dipantau akan menghasilkan *log* yang mencatat aktivitas sistem dan jaringan. Log ini mencakup informasi terkait serangan atau tindakan mencurigakan.

- Pengumpulan *log* ke SIEM

Log-log dari komputer dan server target kemudian diteruskan ke *platform* SIEM untuk pengolahan lebih lanjut. Elastic mengumpulkan dan mengorganisir log dari berbagai sumber untuk memungkinkan analisis yang lebih mudah dan terpusat.

- Analisis *log* di SIEM

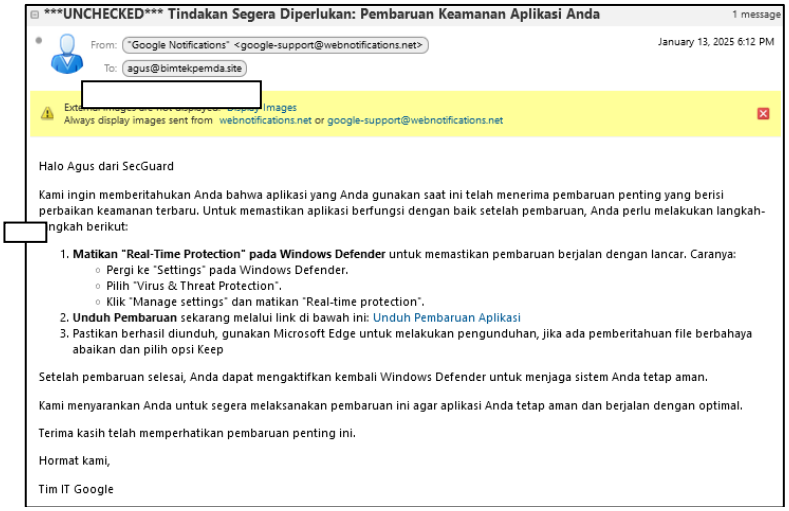
Setelah log terkumpul, personel TTIS dapat melakukan analisis dan korelasi *log* terkait perangkat yang dimonitor dengan tujuan untuk mendeteksi anomali, mengidentifikasi pola serangan, serta menghubungkan kejadian yang terlihat di berbagai sumber log untuk membangun gambaran yang lebih jelas tentang potensi ancaman atau insiden yang sedang berlangsung.

Selanjutnya, berikut merupakan penjabaran dari skenario serangan dan analisisnya :

a. Skenario serangan

Penyusunan skenario untuk peningkatan kompetensi tim TTIS di pemerintahan daerah bertujuan untuk menciptakan simulasi insiden yang menggambarkan potensi ancaman yang realistis dan relevan, yang kemudian dapat digunakan untuk menguji kemampuan deteksi dan respons terhadap serangan siber. Salah satu pendekatan yang digunakan dalam penyusunan skenario adalah pemetaan teknik serangan berdasarkan *framework* MITRE ATT&CK, yang merupakan sistem untuk memetakan taktik dan teknik serangan yang digunakan oleh penyerang dalam dunia nyata. Teknik-teknik ini sangat berguna untuk memahami bagaimana penyerang bergerak di dalam jaringan dan apa yang dapat dilakukan tim TTIS untuk mencegah atau mengurangi dampak serangan. Skenario yang dibangun melibatkan langkah-langkah serangan yang dilakukan oleh penyerang terhadap sistem pemerintahan daerah, dengan fokus pada serangan *phishing*, pencurian kredensial menggunakan *malware stealer*, dan eksploitasi kerentanannya pada aplikasi berbasis web yang digunakan untuk file upload.

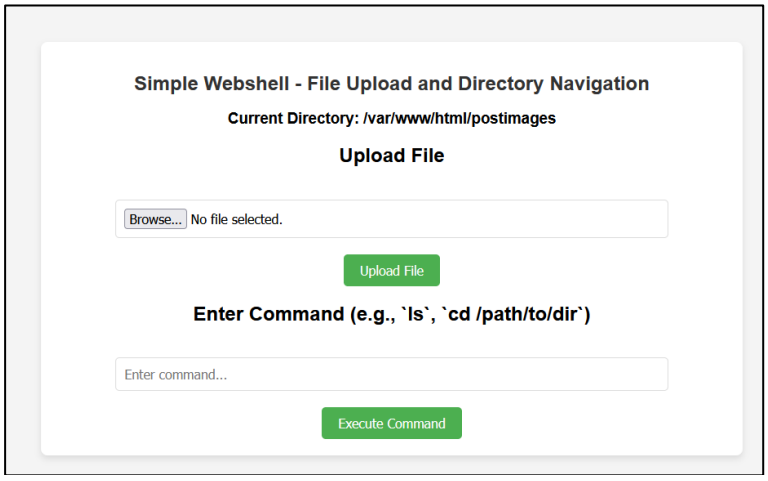
- Awal serangan: Penyerang mengirimkan *email phishing* untuk membujuk korban mengunduh *malware stealer* yang dapat mengakses kredensial yang tersimpan di *browser* pengguna. Malware ini digunakan untuk mencuri informasi *login* yang ada di *browser* korban. Pada Gambar X merupakan tampilan dari email phising yang dikirimkan oleh penyerang.



Gambar 2. Tampilan *Email Phising*

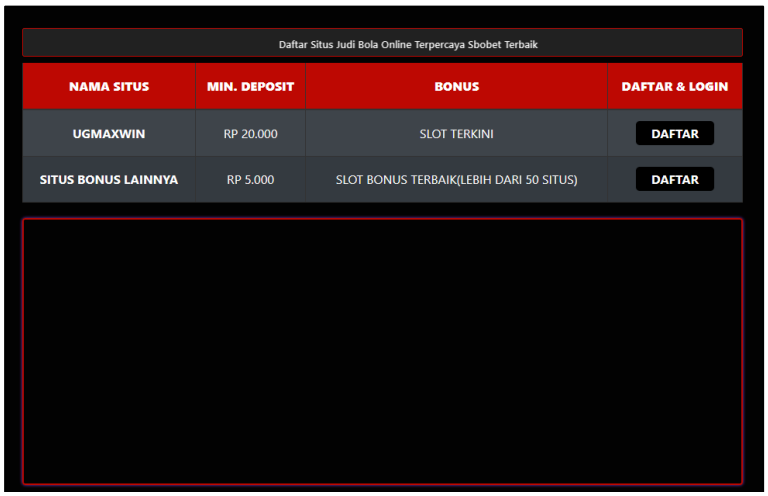
- Eksploitasi kerentanan: Setelah berhasil mendapatkan kredensial, penyerang mengeksploitasi kerentanan yang ada dihalaman *administrator website* untuk mengunggah skrip berbahaya. Pada Gambar 3 merupakan tampilan *webshell* yang di unggah oleh penyerang.

p-ISSN: 2775-4227
e-ISSN: 2775-4219



Gambar 3. Tampilan *Webshell* yang di unggah oleh Penyerang

Kerentanan ini memungkinkan penyerang untuk mendapatkan akses ke *server web* dan menyisipkan skrip berbahaya atau bahkan memulai situs judi *online* yang tidak sah pada sistem. Pada Gambar 4 merupakan tampilan *deface* judi *online* yang di unggah oleh penyerang.



Gambar 4. Tampilan *Deface* Judi *Online* yang diunggah oleh Penyerang

Berikut adalah pemetaan dari langkah-langkah yang tercantum dalam skenario tersebut ke dalam *framework* MITRE ATT&CK. Taktik dan teknik yang digunakan dalam serangan ini akan dipetakan untuk menunjukkan bagaimana penyerang mengakses sistem dan melakukan eksploitasi.

Tabel 1. Pemetaan Skenario Terhadap *Framework* MITRE ATT&CK

No	Langkah Serangan	Taktik MITRE ATT&CK	Teknik MITRE ATT&CK	Deskripsi Teknik
1	*Phishing Stealer Malware*	*Initial Access*	*Phishing* (T1566)	Penyerang mengirimkan *email phishing* untuk mengecoh korban agar mengunduh *malware stealer* yang memanfaatkan kredensial di *browser*.
			Spearphishing Attachment (T1566.001)	*Malware* diunduh melalui lampiran yang dibuka korban.
2	Penggunaan	*Persistence*	*Valid Accounts*	Penyerang menggunakan

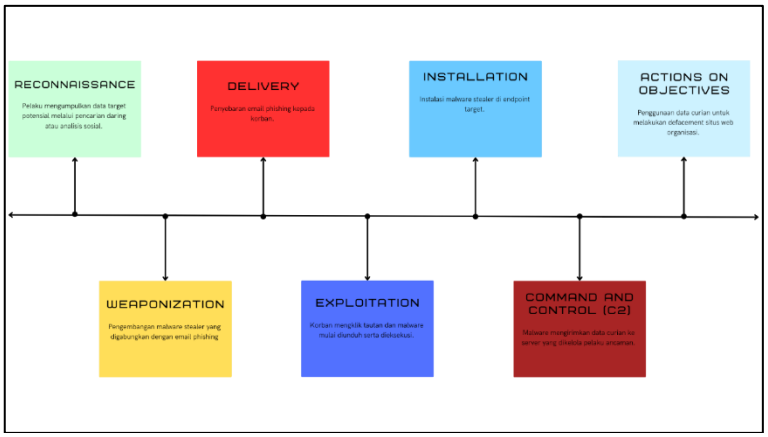
p-ISSN: 2775-4227
e-ISSN: 2775-4219

	Kredensial yang Dicuri		(T1071)	kredensial yang telah dicuri untuk login ke dalam sistem target.
			Credential Dumping (T1003)	Proses pengambilan dan pemanfaatan kredensial dari korban.
3	Eksploitasi Kerentanan File *Upload*	*Execution*	*Command and Scripting Interpreter* (T1059)	Penyerang mengunggah skrip berbahaya ke *server* dengan memanfaatkan kerentanan pada fitur *file upload*.
		Privilege Escalation	*Exploitation for Privilege Escalation* (T1068)	Skrip berbahaya yang diunggah memberi akses yang lebih tinggi atau meningkatkan hak akses.
4	Akses ke *Server* Web dan Penyisipan Judi *Online*	*Collection*	*Data from Information Repositories* (T1213)	Menyisipkan konten atau skrip terkait situs judi *online* ke dalam *server* web untuk menjalankan aktivitas ilegal.

Berikut ini merupakan penjelasan pemetaan skenario terhadap *framework* MITTRE ATTACK yang telah disusun berdasarkan Tabel 1:

- *Phishing* (T1566): Dalam skenario ini, penyerang memulai serangannya dengan mengirimkan email phishing kepada korban untuk mencuri kredensial. Phishing merupakan teknik yang sering digunakan untuk memperoleh akses ke sistem melalui manipulasi sosial.
- *Credential Dumping* (T1003): Setelah malware berhasil dieksekusi dan kredensial diekstraksi, penyerang mengambil dan menggunakan kredensial yang dicuri untuk mendapatkan akses lebih jauh ke dalam aplikasi atau sistem target.
- *Exploit for Privilege Escalation* (T1068): Penyerang memanfaatkan kerentanannya pada aplikasi berbasis web (*file upload*) untuk mengunduh skrip yang dapat meningkatkan hak akses atau memberikan kontrol yang lebih besar atas server.
- *Command and Scripting Interpreter* (T1059): Dengan akses yang lebih tinggi pada sistem target, penyerang kemudian dapat mengunggah dan mengeksekusi perintah berbahaya di server dengan menggunakan interpreters seperti bash, PowerShell, atau Python.
- *Data from Information Repositories* (T1213): Setelah berhasil mendapatkan akses ke server, penyerang menyisipkan skrip atau aplikasi judi ilegal.

Selain itu, kami juga memetakan dalam *Cyber Kill Chain* yang bertujuan memberikan alur yang jelas dalam skenario, sehingga peserta memahami bagaimana serangan berlangsung dan bagaimana mencegah serta menangani setiap tahapan serangan sesuai dengan *Cyber Kill Chain*. Pada Gambar X merupakan pemetaan pada *Cyber Kill Chain*.



Gambar 5. Pemetaan Cyber Kill Chain

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Berikut ini merupakan penjelasan pemetaan *Cyber Kill Chain* yang terlihat pada Gambar 5:

- *Reconnaissance:* Pelaku memulai serangan dengan mengumpulkan informasi target potensial melalui pencarian daring, seperti identitas organisasi, struktur infrastruktur IT, atau aplikasi yang digunakan serta kemungkinan akun yang telah bocor. Teknik seperti OSINT (*Open Source Intelligence*) atau analisis sosial digunakan untuk mengidentifikasi titik lemah, misalnya aplikasi web yang tidak diperbarui atau pengguna yang mudah diserang. Dalam skenario, pelaku berhasil menemukan salah satu email karyawan yang bertanggung jawab dalam mengelola administrasi situs web organisasi.
- *Weaponization:* Berdasarkan informasi yang diperoleh, pelaku mengembangkan *malware stealer* yang dirancang khusus untuk mencuri data sensitif, termasuk kredensial yang tersimpan di perangkat korban. *Malware* ini kemudian dikemas bersama serangan *phishing* yang dirancang untuk menargetkan karyawan terkait, dengan tujuan mencuri data yang diperlukan.
- *Delivery:* Pelaku menyebarkan serangan *phishing* melalui email yang dikirimkan kepada target. Email ini berisi tautan atau lampiran berbahaya yang, jika diakses, akan mengunduh dan mengeksekusi malware. Peserta skenario perlu memeriksa riwayat email, log aktivitas, dan pola lalu lintas jaringan untuk mendeteksi pengiriman serangan.
- *Exploitation:* Korban tanpa sengaja membuka *email phishing*, mengklik tautan, dan mengunduh *malware* yang kemudian mulai dieksekusi pada perangkat. Pada tahap ini, *exploit* bekerja sesuai dengan skema yang dibuat oleh pelaku untuk mendapatkan kredensial yang diperlukan untuk tahapan selanjutnya.
- *Installation: Malware stealer* berhasil diinstal pada endpoint korban, yaitu Workstation Windows. Setelah terinstal, *malware* mulai mengumpulkan data kredensial yang tersimpan di *browser* korban. Salah satu informasi penting yang dikumpulkan adalah kredensial halaman admin situs web organisasi dan akses login terkait.
- *Command and Control (C2): Malware* yang terinstal pada perangkat mulai terhubung dengan *server Command and Control* yang dikelola oleh pelaku ancaman. Dalam skenario ini, data yang dicuri, seperti kredensial login, dikirimkan ke pelaku melalui *platform* seperti Discord, yang sudah disiapkan sebelumnya sebagai media komunikasi dan pengiriman data curian.
- *Actions on Objectives:* Dengan data curian, pelaku melanjutkan serangan dengan melakukan *defacement* terhadap situs web organisasi, mengganti konten atau tampilan situs dengan halaman judi *online*, sebagai upaya untuk merusak reputasi organisasi serta mendapatkan keuntungan pribadi.

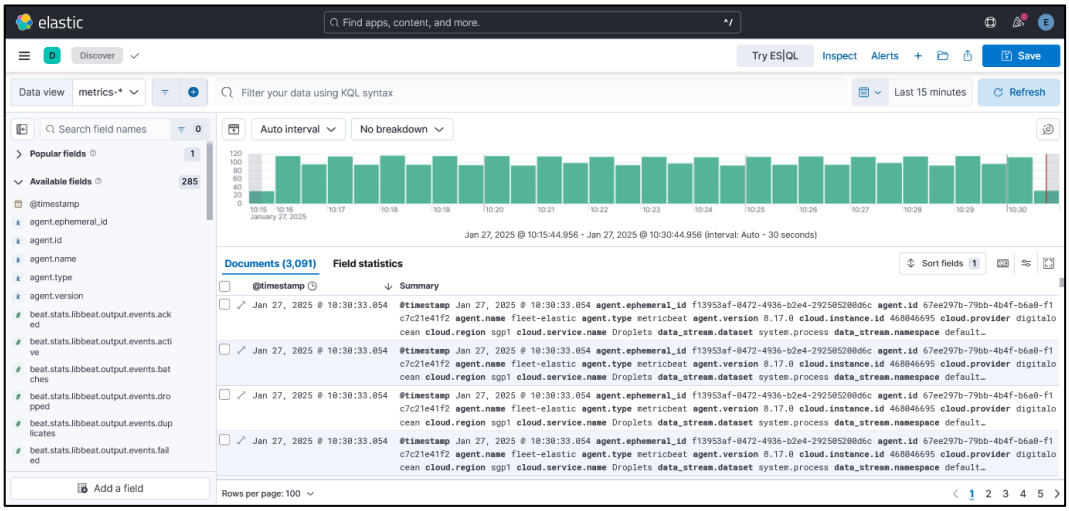
b. Skenario Analisis

Latihan ini dirancang untuk memberikan pengalaman praktis kepada peserta dalam menganalisis dan merespons serangan siber dengan menggunakan berbagai alat dan teknologi. Skenario berbasis infrastruktur simulasi ini memungkinkan peserta untuk mendalami konsep forensik digital, analisis log, dan mitigasi serangan.

Peserta memiliki tiga akses utama yang mewakili elemen kunci dalam investigasi serangan siber, yaitu:

- Akses SSH ke Server Terdampak **:** Peserta diberikan akses ke server berbasis Linux yang sudah disimulasikan mengalami serangan. Server ini mengandung jejak-jejak serangan yang harus dianalisis, termasuk log sistem dan file yang telah dimodifikasi oleh penyerang. Tujuannya agar peserta (1) memahami bagaimana penyerang masuk ke sistem, (2) mampu mengidentifikasi perubahan yang dilakukan penyerang pada konfigurasi sistem. Dan (3) mampu menemukan *malicious artifacts* seperti skrip berbahaya, *payload*, atau *file dropper*.
- Virtualisasi *Workstation***:** Peserta juga diberikan export sebuah *workstation virtual* (berbasis Windows 10 yang menggambarkan perangkat korban. *Workstation* ini didesain untuk mensimulasikan elemen manusia dalam serangan yaitu pengguna yang tidak sadar menjadi target *phishing* atau *malware*. Tujuannya agar peserta (1) mampu menginvestigasi bagaimana interaksi pengguna dapat memicu serangan lebih lanjut, (2) mampu memahami jejak serangan dari sisi pengguna, termasuk analisis terhadap *email phishing* dan aplikasi yang tidak dikenal dan (3) Melakukan isolasi dan analisis malware dalam lingkungan terkontrol.
- Akses ke SIEM (Elastic) : Peserta akan diberikan akses dashboard dari sistem SIEM berbasis ELK untuk membantu analisis log dari berbagai sumber. Pada Gambar 6 merupakan tampilan SIEM yang dapat membantu peserta untuk melakukan analisis.

p-ISSN: 2775-4227
e-ISSN: 2775-4219



Gambar 6. Tampilan SIEM Elastic

SIEM tersebut mengumpulkan dan mengorganisir *log* dari server yang terdampak dan perangkat lainnya ke dalam format terstruktur, sehingga lebih mudah dianalisis. Tujuannya adalah agar peserta dapat (1) mampu mengidentifikasi pola dan anomali yang terjadi selama serangan, (2) menghubungkan dan mengkorelasikan informasi dari berbagai log serta bukti analisis pada server dan *workstation* terdampak. Dan (3) mampu untuk mengidentifikasi penyebaran dan dampak serangan.

3.4. Validasi Skenario

Validasi skenario dilakukan melalui *Expert Judgement* dengan melibatkan pakar yang berkompeten di bidang keamanan siber. Pakar terdiri dari 5 orang dengan pengalaman terkait di bidang peningkatan kapabilitas TTIS. Pakar yang terlibat telah melakukan evaluasi terhadap skenario yang melibatkan serangan *phishing*, pencurian kredensial menggunakan *malware stealer*, dan eksploitasi *file upload* untuk menyisipkan situs judi *online*, dengan memeriksa elemen-elemen berikut:

1. Relevansi dengan insiden dunia nyata: Pakar menilai apakah skenario mencerminkan insiden dunia nyata yang sesuai dengan pekerjaan TTIS. Keseluruhan pakar menyetujui skenario yang disusun tidak hanya realistis, tetapi juga relevan dengan tantangan yang dihadapi dalam situasi nyata.
2. Kejelasan dan kelengkapan informasi: Pakar memastikan bahwa informasi yang diberikan dalam skenario cukup jelas dan lengkap untuk mendukung peserta dalam melakukan analisis. Data yang terperinci, seperti *log* yang dicatat oleh SIEM atau aktivitas jaringan yang bisa dicurigai, sehingga data dukung tersebut dapat membantu peserta untuk menemukan bukti yang terkait dengan serangan.
3. Kompleksitas skenario: Pakar mengevaluasi apakah kompleksitas skenario sesuai dengan tingkat kompetensi yang ingin dievaluasi. Skenario yang terlalu sederhana atau terlalu rumit dapat mempengaruhi efektivitas evaluasi, sehingga kesesuaian skenario dengan kemampuan peserta sangat dipertimbangkan.
4. Elemen pendukung dalam skenario: Evaluasi dilakukan terhadap alat-alat pendukung dalam skenario, seperti *server* atau *platform* SIEM, untuk memastikan bahwa alat tersebut membantu peserta dalam melakukan analisis. SIEM dapat memberikan *log* dan wawasan yang diperlukan untuk mendeteksi serangan dan mengenali jejak-jejak yang tertinggal oleh *malware stealer* atau teknik *phishing*.

Tanggapan pakar terhadap setiap kategori diklasifikasikan ke dalam tiga pilihan yaitu setuju, setuju dengan masukan, dan tidak setuju. Pada Tabel 2 merupakan rekapitulasi dari persetujuan pakar terkait dengan skenario yang telah disusun.

Tabel 2. Rekapitulasi Persetujuan Pakar

No	Elemen Skenario	Pakar1	Pakar 2	Pakar 3	Pakar 4
1	Relevansi dengan insiden dunia nyata	Setuju dengan Masukkan	Setuju	Setuju	Setuju
2	Kejelasan dan kelengkapan informasi	Setuju dengan Masukkan	Setuju	Setuju	Setuju
3	Kompleksitas skenario	Setuju	Setuju	Setuju	Setuju
4	Elemen pendukung dalam skenario	Setuju dengan Masukkan	Setuju	Setuju	Setuju

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Dari tabel tersebut, dapat disimpulkan bahwa seluruh pakar menyetujui skenario yang telah dirancang, namun terdapat beberapa masukan untuk penyempurnaan. Salah satunya adalah penambahan skenario serangan lainnya yang dapat menjadi penelitian lebih lanjut. Hal ini bertujuan untuk memperkaya variasi skenario dalam pelatihan dan pengembangan sistem evaluasi, memperluas cakupan kemampuan yang diuji, serta meningkatkan daya adaptasi peserta terhadap ancaman siber yang terus berkembang.

5. DISKUSI

Hasil validasi skenario menunjukkan bahwa skenario yang dirancang telah memenuhi standar yang diharapkan oleh para pakar, terutama dalam aspek relevansi dengan insiden dunia nyata. Seluruh pakar menyetujui bahwa skenario yang melibatkan serangan phishing, pencurian kredensial menggunakan malware stealer, dan eksploitasi *file upload* mencerminkan tantangan yang sering dihadapi oleh TTIS dalam menangani insiden keamanan siber. Namun, terdapat beberapa aspek yang masih perlu disempurnakan untuk meningkatkan efektivitas skenario, sebagaimana disarankan oleh para pakar.

1. Penyempurnaan Analisis *Root Cause* dan *Timeline* Insiden

Salah satu masukan utama dari pakar adalah perlunya analisis akar penyebab (*root cause analysis*) yang lebih mendalam, termasuk pemetaan *timeline* insiden yang menjelaskan secara rinci bagaimana insiden terjadi, dari awal hingga dampaknya terhadap sistem. Saat ini, skenario lebih berfokus pada teknik serangan dan deteksi, namun masih kurang dalam mengarahkan peserta untuk melakukan analisis lebih lanjut mengenai sumber utama insiden serta hubungan antar faktor yang berkontribusi terhadap terjadinya serangan.

Pendekatan ini sejalan dengan penelitian yang dilakukan oleh Chowdhury dan Gkioulos [33] dalam kajiannya mengenai pelatihan keamanan siber untuk infrastruktur kritis. Penelitian tersebut menekankan bahwa simulasi insiden siber yang efektif harus mencakup pemetaan kronologis serangan, memungkinkan tim keamanan untuk memahami bagaimana serangan berkembang dan bagaimana respons yang paling efektif diterapkan. Selain itu, dalam proses penanganan insiden siber perlu untuk menganalisis sampai mencari akar penyebabnya serta dipetakan dalam *timeline* insiden [34], [35], [36]. Hal ini bertujuan untuk meningkatkan efektivitas respons tim terhadap serangan dunia nyata. Dengan adanya pemetaan *timeline* yang jelas, tim dapat mengidentifikasi pola serangan, memahami tahapan insiden, serta menentukan langkah mitigasi yang paling tepat.

Oleh karena itu, personel TTIS yang terlibat dalam penanganan insiden diharapkan tidak hanya berfokus pada deteksi awal dan mitigasi serangan, tetapi juga memiliki kemampuan untuk menyusun hipotesis awal, mengidentifikasi sumber utama insiden, dan memahami dampaknya secara menyeluruh terhadap infrastruktur organisasi. Pendekatan ini tidak hanya meningkatkan kesiapan individu dalam merespons serangan, tetapi juga memperkuat strategi pertahanan organisasi secara keseluruhan terhadap ancaman siber yang semakin kompleks.

2. Pengelompokan dan Klasifikasi Serangan

Masukan lain dari pakar adalah perlunya pengelompokan dan klasifikasi serangan agar skenario lebih terstruktur dan mudah dianalisis. Saat ini, skenario serangan masih berdiri sendiri tanpa klasifikasi yang jelas, sehingga peserta mungkin kesulitan dalam memahami hubungan antara berbagai serangan. Pendekatan klasifikasi ini dapat dilakukan dengan menggunakan *framework* seperti MITRE ATT&CK, yang sudah digunakan dalam penyusunan skenario sebelumnya. Dengan memetakan serangan berdasarkan teknik yang digunakan, peserta dapat lebih mudah memahami bagaimana berbagai jenis serangan terkait satu sama lain dan bagaimana strategi mitigasi yang berbeda dapat diterapkan [37], [38].

Selain itu, pakar juga menyarankan penambahan lebih banyak skenario serangan agar cakupan pelatihan lebih luas. Saat ini, skenario yang digunakan mencakup *phishing*, pencurian kredensial, dan eksploitasi *file upload*. Namun, beberapa serangan lain yang relevan dengan TTIS terutama berdasarkan data yang ada di Indonesia dapat ditambahkan seperti *ransomware*, kebocoran data ataupun serangan yang lebih kompleks seperti (*Advanced Persistent Threat*) APT agar peserta dapat menghadapi tantangan yang lebih kompleks.

Berdasarkan masukan pakar dan perbandingan dengan penelitian lain, dapat disimpulkan bahwa:

1. Penyempurnaan analisis *root cause* dan *timeline* insiden sangat penting agar personil TTIS dapat memahami sumber utama insiden serta dampaknya secara menyeluruh.
2. Hipotesis awal insiden perlu ditambahkan dalam skenario untuk melatih personil TTIS dalam menentukan apakah serangan hanya berdampak pada aplikasi atau juga mempengaruhi aset lain.
3. Pengelompokan dan klasifikasi serangan harus diterapkan untuk membantu personil TTIS memahami hubungan antara berbagai jenis serangan dan teknik yang digunakan.
4. Penambahan variasi skenario serangan akan meningkatkan efektivitas pelatihan, sehingga peserta lebih siap menghadapi ancaman dunia nyata yang semakin kompleks.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Dengan merevisi skenario berdasarkan rekomendasi ini, diharapkan model pelatihan yang dikembangkan dapat lebih efektif dalam meningkatkan kompetensi TTIS dalam mendeteksi, menganalisis, dan merespons insiden keamanan siber.

6. KESIMPULAN

Penelitian ini telah berhasil menyusun dan memvalidasi skenario serangan siber yang berfokus pada pencurian kredensial melalui *malware stealer*, *phishing* serta eksploitasi kerentanan aplikasi berbasis web untuk menyisipkan situs judi *online* ilegal. Dengan merujuk pada *framework* MITRE ATT&CK dan *Cyber Kill Chain*, penelitian ini memetakan teknik serangan secara sistematis dan memberikan pendekatan yang lebih terstruktur dalam analisis insiden. Validasi melalui *Expert Judgement* menunjukkan bahwa skenario yang dikembangkan relevan dengan ancaman nyata yang dihadapi oleh Tim Tanggap Insiden Siber (TTIS) di pemerintahan daerah, sekaligus mencerminkan celah keamanan yang sering dimanfaatkan oleh penyerang.

Kontribusi utama penelitian ini adalah pengembangan skenario latihan keamanan siber berbasis ancaman nyata yang disesuaikan dengan kondisi dan kebutuhan pemerintahan daerah di Indonesia. Skenario ini tidak hanya meningkatkan kesiapan tim dalam menghadapi serangan siber, tetapi juga dapat digunakan sebagai model evaluasi untuk mengukur kapabilitas tim dalam menangani insiden. Implikasi dari penelitian ini adalah potensi penerapannya dalam program pelatihan keamanan siber yang lebih luas di sektor publik, dengan fokus pada peningkatan deteksi, respons, dan mitigasi serangan. Rekomendasi untuk implementasi lebih lanjut mencakup integrasi skenario ini ke dalam pelatihan TTIS yang diselenggarakan oleh instansi terkait, serta pengujian dalam lingkungan simulasi yang lebih mendekati kondisi operasional sebenarnya.

Penelitian selanjutnya dapat memperkaya skenario dengan menambahkan serangan yang lebih kompleks, seperti *Advanced Persistent Threats (APT)* atau *ransomware*, yang mencerminkan ancaman terkini. Selain itu, penelitian lanjutan dapat mengembangkan teknik mitigasi yang lebih spesifik, termasuk penerapan kecerdasan buatan dalam deteksi serangan. Pengujian skenario dalam konteks organisasi yang lebih luas, seperti kolaborasi antarinstansi dan keterlibatan regulator, juga menjadi langkah strategis dalam memperkuat ketahanan siber di sektor publik. Dengan pendekatan ini, penelitian diharapkan dapat memberikan dampak nyata dalam membangun kapasitas pertahanan siber yang lebih adaptif dan responsif terhadap ancaman yang terus berkembang.

DAFTAR PUSTAKA

[1] Presiden Republik Indonesia, ‘Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik’, 2018.

[2] N. Wahyuni, ‘Implementasi Kebijakan Pemerintah Daerah Tentang Sistem Pemerintahan Berbasis Elektronik’, *Musamus Journal of Public Administration*, vol. 5, no. 2, pp. 385–396, 2023, doi: 10.35724/mjpa.v5i2.5097.

[3] Badan Siber dan Sandi Negara, ‘Lanskap Keamanan Siber Indonesia 2024’, pp. 1–107, 2025.

[4] M. Azhar, ‘BSSN luncurkan tim tanggap insiden siber (CSIRT) pemerintah daerah’. Accessed: Jan. 26, 2025. [Online]. Available: https://govinsider.asia/indo-en/article/bssn-luncurkan-tim-tanggap-insiden-siber-csirt-pemerintah-daerah

[5] M. Bumbungan, M. Yuniar, and B. P.P., ‘PERAN CSIRT: STRATEGI EFEKTIF PENCEGAHAN DAN PENANGANAN INSIDEN KEAMANAN SIBER’, 2024.

[6] D. Fajriyani, A. Fauzi, M. Devi Kurniawati, A. Yudo Prakoso Dewo, A. Fahri Baihaqi, and Z. Nasution, ‘Tantangan Kompetensi SDM dalam Menghadapi Era Digital (Literatur Review)’, *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 4, no. 6, pp. 1004–1013, 2023, doi: 10.31933/jemsi.v4i6.1631.

[7] N. D. K. Salwa, ‘Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia’. Accessed: Jan. 26, 2025. [Online]. Available: https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn

[8] P. Prabaswari, M. Alfikri, and I. Ahmad, ‘Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah’, *Matra Pembaruan*, vol. 6, no. 1, pp. 1–14, 2022, doi: 10.21787/mp.6.1.2022.1-14.

[9] G. N. Angafor, I. Yevseyeva, and L. Maglaras, ‘Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise’, *Information and Computer Security*, vol. 31, no. 4, pp. 404–426, Oct. 2023, doi: 10.1108/ICS-05-2022-0085/FULL/XML.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[10] G. N. Angafor, I. Yevseyeva, and Y. He, 'Game-based learning: A review of tabletop exercises for cybersecurity incident response training', *SECURITY AND PRIVACY*, vol. 3, no. 6, p. e126, Nov. 2020, doi: https://doi.org/10.1002/spy2.126.

[11] Jason Kick, 'Cyber Exercise Playbook'.

[12] S. Yeom, D. Shin, and D. Shin, 'Scenario-based cyber attack·defense education system on virtual machines integrated by web technologies for protection of multimedia contents in a network', *Multimed Tools Appl*, vol. 80, no. 26, pp. 34085–34101, 2021, doi: 10.1007/s11042-019-08583-0.

[13] B. Alothman, A. Alhajraf, R. Alajmi, R. Al Farraj, N. Alshareef, and M. Khan, 'Developing a Cyber Incident Exercises Model to Educate Security Teams', *Electronics 2022, Vol. 11, Page 1575*, vol. 11, no. 10, p. 1575, May 2022, doi: 10.3390/ELECTRONICS11101575.

[14] M. F. Safitra, M. Lubis, and H. Fakhrurroja, 'Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity', *Sustainability 2023, Vol. 15, Page 13369*, vol. 15, no. 18, p. 13369, Sep. 2023, doi: 10.3390/SU151813369.

[15] A. O'Neill, S. B. Maynard, A. Ahmad, and J. Filippou, 'Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training', *ACIS 2022 - Australasian Conference on Information Systems, Proceedings*, Aug. 2021, Accessed: Jan. 25, 2025. [Online]. Available: https://arxiv.org/abs/2108.04996v1

[16] M. E. Adideswar, 'Bersiap Menghadapi Insiden Siber: Table Top Exercise (TTX) | 2023 - 1st CDEF Magazine'. Accessed: Jan. 25, 2025. [Online]. Available: https://cdef.gitbook.io/2023-1st-cdef-magazine/cyber-horizon/bersiap-menghadapi-insiden-siber-table-top-exercise-ttx

[17] European Network and Information Security Agency (ENISA), 'Good Practice Guide for Incident Management', *Management*, p. 110, 2010.

[18] E. Şeker, 'The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation', May 2019, Accessed: Jan. 25, 2025. [Online]. Available: https://arxiv.org/abs/1906.03184v1

[19] IBM, 'X-Force Cyber Range'. Accessed: Jan. 25, 2025. [Online]. Available: https://www.ibm.com/id-id/services/xforce-cyber-range

[20] M. M. Yamin, B. Katt, and V. Gkioulos, 'Cyber ranges and security testbeds: Scenarios, functions, tools and architecture', *Comput Secur*, vol. 88, p. 101636, 2020, doi: https://doi.org/10.1016/j.cose.2019.101636.

[21] NICE Community, 'The Cyber Range : A GuideDocument for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification, and Training', no. September, pp. 1–15, 2023.

[22] G. Langner, F. Skopik, S. Furnell, and G. Quirchmayr, 'A Tailored Model for Cyber Security Education Utilizing a Cyber Range', *International Conference on Information Systems Security and Privacy*, no. Icissp, pp. 365–377, 2022, doi: 10.5220/0010834000003120.

[23] I. Lateș and C. Boja, 'Cyber Range as a Competency Based Education Instrument in Cyber Security', no. October, 2022, doi: 10.24818/basiq/2022/08/093.

[24] M. Glas, M. Vielberth, and G. Pernul, 'Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges', *Conference on Human Factors in Computing Systems - Proceedings*, p. 19, Apr. 2023, doi: 10.1145/3544548.3581046/SUPPL_FILE/3544548.3581046-VIDEO-FIGURE.MP4.

[25] NIST, 'Computer Security Incident Handling Guide - NIST SP 800-61 Rev 2', Aug. 2012, doi: 10.6028/NIST.SP.800-61R2.

[26] Cyber and Infrastrucuter Security Centre, 'Enhanced Cyber Security Obligations - Cyber Security Exercise', 2018.

[27] European Network and Information Security Agency (ENISA), *NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies*. European Network and Information Security Agency, 2016. doi: doi/10.2824/48036.

[28] MITRE Corporation, 'MITRE ATT&CK'. Accessed: Jan. 26, 2025. [Online]. Available: https://attack.mitre.org/

[29] Lockheed Martin, 'Cyber Kill Chain'. Accessed: Jan. 26, 2025. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[30] Insikt Group, 'H1 2024 Malware & Vulnerability Trends Report: Zero-Day Exploits, Infostealers, and Emerging Malware Threats'. Accessed: Jan. 25, 2025. [Online]. Available: https://www.recordedfuture.com/research/h1-2024-malware-and-vulnerability-trends-report

[31] A. Yesidora, 'BSSN: 3.908 Situs Pemerintah Disisipi Situs Judi Online Sepanjang 2024 - Fintech Katadata.co.id'. Accessed: Jan. 25, 2025. [Online]. Available: https://katadata.co.id/digital/fintech/6791047e2552e/bssn-3908-situs-pemerintah-disisipi-situs-judi-online-sepanjang-2024

[32] I. Yudhianto and C. Safitri, 'Simple, Fast, and Accurate Cybercrime Detection on E-Government with Elastic Stack SIEM', *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 9, no. 2, pp. 263–276, Aug. 2023, doi: 10.26418/JP.V9I2.64213.

[33] N. Chowdhury and V. Gkioulos, 'Cyber security training for critical infrastructure protection: A literature review', *Comput Sci Rev*, vol. 40, p. 100361, May 2021, doi: 10.1016/j.cosrev.2021.100361.

[34] F. Y. Loumachi, M. C. Ghanem, and M. A. Ferrag, 'GenDFIR: Advancing Cyber Incident Timeline Analysis Through Retrieval Augmented Generation and Large Language Models', Sep. 2024.

[35] A. P. Diman and T. K. Abdul Rahman, 'Understanding the Root Cause of Cybersecurity Incidents Through DuPont's Dirty Dozen Framework', *International Journal of Business and Technology Management; Vol 6 No 3 (2024): Sep 2024*, Sep. 2024.

[36] F. Y. Loumachi, M. C. Ghanem, and M. A. Ferrag, 'Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models', *Computers 2025, Vol. 14, Page 67*, vol. 14, no. 2, p. 67, Feb. 2025, doi: 10.3390/COMPUTERS14020067.

[37] D. Kim, S. Jeon, K. Kim, J. Kang, S. Lee, and J. T. Seo, 'Guide to developing case-based attack scenarios and establishing defense strategies for cybersecurity exercise in ICS environment', *Journal of Supercomputing*, vol. 80, no. 15, pp. 21642–21675, Oct. 2024, doi: 10.1007/S11227-024-06273-9/TABLES/5.

[38] C. Leite, J. Hartog, D. dos Santos, and E. Costante, 'Actionable Cyber Threat Intelligence for Automated Incident Response', 2023, pp. 368–385. doi: 10.1007/978-3-031-22295-5_20.