Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Analisis Efektivitas Penerapan *Cyber Threat Intelligence* Dalam Upaya Pencegahan Serangan Siber di Lingkup Badan Pengusahaan Batam (Bp Batam)

Surya Saputra [1], Maidel Fani [2],
Program Studi Rekayasa Keamanan Siber
Jurusan Teknik Informatika, Politeknik Negeri Batam
suryasptr1910@gmail.com [1], maidelfani@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

Cyber Threat Intelligence, OpenCTI, Threat Hunting, Government Sector, Cybersecurity

ABSTRACT

The increasing complexity of cyber threats targeting government institutions has driven the need for a more proactive and intelligence-based defense approach. Batam Indonesia Free Zone Authority (BP Batam), as a strategic governmental agency, has faced a significant rise in cyber threats, particularly spyware, phishing, and DNS-based exploitation. This study analyses the effectiveness of Cyber Threat Intelligence (CTI) implementation using the OpenCTI platform in enhancing BP Batam's cybersecurity operations. A qualitative method with a phenomenological approach was used, involving in-depth interviews with cybersecurity professionals at BP Batam and observations of the customized OpenCTI system. The findings indicate that CTI implementation significantly improves threat detection, incident response speed, and contextual awareness of threat actors and attack techniques. The integration of OpenCTI supported by external threat feeds and visual correlation of Indicators of Compromise (IOC) has shifted BP Batam's security posture from reactive to intelligence driven. Although system integration is still partially manual, CTI usage has enhanced threat hunting capability and risk management strategies by aligning with the MITRE ATT&CK framework. The study concludes that OpenCTI supports the development of a more adaptive and data-driven cybersecurity strategy in the public sector.

I. PENDAHULUAN

Dalam beberapa tahun terakhir, serangan siber yang menargetkan instansi pemerintahan di Indonesia menunjukkan peningkatan baik dari segi frekuensi maupun kompleksitas. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2023 tercatat sebanyak 103 insiden dugaan kebocoran data, dengan sektor administrasi pemerintahan menjadi yang paling terdampak (71 kasus), diikuti oleh sektor keuangan (12 kasus) [1]. Jenis serangan yang paling umum meliputi *spyware*, *phishing*, dan eksploitasi berbasis *DNS*, yang mengindikasikan perlunya pendekatan keamanan siber yang lebih proaktif, khususnya di lembaga strategis seperti Badan Pengusahaan Batam (BP Batam) [2].

Cyber Threat Intelligence (CTI) merupakan pendekatan strategis dalam mengelola dan menganalisis informasi ancaman siber guna mendukung deteksi dini, mitigasi risiko, dan respons insiden secara tepat [3]. Salah satu komponen penting dalam *CTI* adalah *Indicator of Compromise* (*IOC*), yaitu artefak teknis seperti alamat *IP, hash file*, atau *domain* mencurigakan yang menunjukkan potensi terjadinya kompromi pada sistem [4], [5], Untuk mengelola informasi tersebut secara terstruktur, organisasi dapat menggunakan *Threat Intelligence Platform (TIP),* yakni sistem yang mengintegrasikan berbagai sumber data ancaman (*threat feeds*), mengkorelasikan antarindikator, dan mengaitkan temuan dengan kerangka kerja serangan seperti *MITRE ATT&CK* [6], [7]

OpenCTI adalah salah satu *platform CTI* bersifat *open-source* yang memungkinkan organisasi untuk mengelola *IOC,* memvisualisasikan hubungan antar-entitas ancaman, serta menghubungkannya dengan taktik dan teknik serangan [8], [9],[10]. Penelitian terdahulu menunjukkan bahwa

e-ISSN: 2548-6861

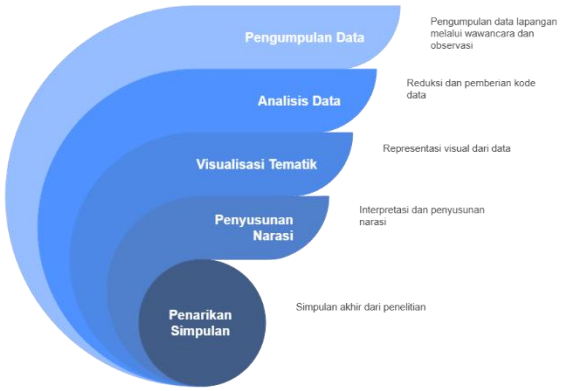
implementasi *CTI* dapat meningkatkan efektivitas operasi keamanan siber, baik dari sisi deteksi, manajemen risiko, hingga pemetaan aktivitas *threat actor* [7], [10]. Namun, studi terkait penerapan *CTI* di sektor pemerintahan Indonesia masih sangat terbatas, terutama dalam hal integrasi *IOC* secara sektoral, adopsi *dashboard* intelijen, serta pemanfaatan informasi dalam proses *threat hunting* yang kontekstual.

Penelitian ini bertujuan untuk menganalisis efektivitas penerapan *Cyber Threat Intelligence* menggunakan *platform OpenCTI* dalam mendukung deteksi dan mitigasi serangan siber di lingkungan BP Batam. Diharapkan hasil dari penelitian ini dapat berkontribusi dalam merumuskan strategi pertahanan siber berbasis intelijen di lingkungan pemerintahan, serta menjadi referensi praktis dalam integrasi *platform CTI* secara efektif di lingkungan institusi publik.

II. METODE

Penelitian ini dilaksanakan dengan menggunakan metode kualitatif yang berlandaskan pada pendekatan fenomenologis [11], yang bertujuan untuk menggali dan memahami pengalaman, pemaknaan, serta persepsi praktisi keamanan siber terhadap penerapan *Cyber Threat Intelligence (CTI)* di lingkungan Badan Pengusahaan Batam (BP Batam). Pendekatan ini memungkinkan peneliti mengeksplorasi secara mendalam realitas yang dialami subjek secara langsung [12], termasuk bagaimana *CTI* memberikan dampak pada proses deteksi dan mitigasi ancaman.

Penelitian dilaksanakan melalui tahapan yang mencakup perumusan masalah, pengumpulan data lapangan, observasi sistem *CTI*, analisis data secara tematik, hingga penarikan simpulan dari hasil wawancara dan sistem dokumentasi teknis [13]. Proses ini divisualisasikan dalam Gambar 1 berikut:



Gambar 1. Alur proses penelitian

Setiap tahapan dilakukan secara sistematis dan berorientasi pada pemahaman makna yang dibentuk dari pengalaman para informan.

A. Desain Penelitian

Penelitian ini dilakukan pada periode Maret-Juni 2025, dengan ruang lingkup pada unit sub bidang keamanan TI di BP Batam. Teknik yang digunakan dalam pengumpulan data adalah wawancara mendalam dengan format semi-terstruktur terhadap tiga narasumber utama yaitu, Kepala Keamanan TI BP Batam, *Cyber Security Analyst*, dan *Application Security Engineer*. Teknik *purposive sampling* digunakan dalam pemilihan informan, dengan mempertimbangkan keterlibatan langsung mereka dalam pengelolaan keamanan sistem dan implementasi *CTI.*

Wawancara direkam dan ditranskrip untuk dianalisis secara tematik. Selain itu, dilakukan observasi langsung terhadap *dashboard OpenCTI* yang telah dikustomisasi serta pengumpulan data teknis dari sistem pendukung seperti *firewall, IDS/IPS, WAF*, dan *SIEM.* Untuk meningkatkan validitas, diterapkan triangulasi data melalui perbandingan antara hasil wawancara, observasi sistem, dan log aktivitas teknis lapangan

B. Teknik Pengumpulan Data

Data dikumpulkan melalui tiga metode utama yang dirancang untuk saling melengkapi satu sama lain, yaitu wawancara semi-terstruktur, observasi sistem, dan dokumentasi teknis. Kombinasi dari ketiga metode ini dimanfaatkan untuk menggali informasi dari beragam sumber dan sudut pandang yang berbeda. Triangulasi dilakukan untuk meningkatkan validitas internal, yaitu dengan membandingkan dan mengkonfirmasi silang data dari hasil wawancara, observasi langsung terhadap sistem *OpenCTI,* serta dokumentasi teknis dan *log* aktivitas sistem [14].

Teknik pengumpulan data yang diterapkan dalam penelitian ini mencakup:

1) *Wawancara Semi-Terstruktur:* Wawancara dilakukan terhadap tiga informan kunci, yaitu Kepala Keamanan TI, Analis Keamanan Siber, dan *Application Security Engineer* di lingkungan BP Batam. Teknik purposive sampling digunakan dalam menentukan informan yang relevan dengan tujuan penelitian.

Jumlah tiga narasumber dianggap mencukupi untuk penelitian fenomenologis, karena fokus utamanya adalah pada kedalaman eksplorasi makna pengalaman, bukan pada kuantitas partisipan. Moustakas menjelaskan bahwa dalam pendekatan fenomenologi, peneliti dapat bekerja dengan jumlah narsumber kecil asalkan memiliki pengalaman langsung terhadap fenomena yang diteliti [15]. Hal ini juga diperkuat oleh Creswell yang merekomendasikan 3 hingga 10 partisipan dalam studi fenomenologi [16].

Kriteria pemilihan informan ditentukan berdasarkan indikator:

- Profesional di bidang keamanan siber
- Terlibat langsung dalam pengelolaan dan penerapan *CTI*
- Memahami sistem keamanan TI yang digunakan di BP Batam

- Memiliki wawasan terhadap insiden keamanan siber yang pernah terjadi

Pertanyaan wawancara disusun berdasarkan lima indikator efektivitas CTI yang diadaptasi dari penelitian sebelumnya [3]. Setiap sesi berlangsung selama 30-60 menit dengan pendekatan semi-terstruktur, yang memungkinkan eksplorasi terbuka namun tetap terarah terhadap fokus penelitian.

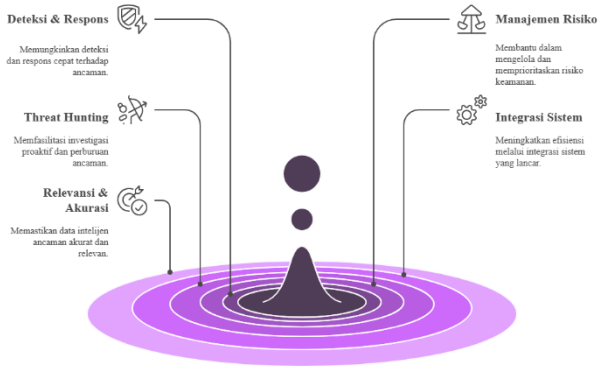
2) Observasi Sistem: Peneliti melakukan observasi langsung terhadap implementasi *OpenCTI.* Observasi difokuskan pada alur kerja sistem, pemanfaatan konektor, proses *update IOC* harian, serta penggunaan dashboard untuk visualisasi *threat actor, malware*, dan domain berbahaya. Hal ini membantu peneliti memahami secara teknis bagaimana sistem bekerja dan digunakan dalam konteks operasional.

3) Dokumentasi Teknis: Dokumen pendukung seperti tangkapan layar sistem, konfigurasi konektor, *log* dari *firewall* dan *IDS*, serta hasil output *IOC* dikumpulkan untuk memperkuat data primer dari wawancara. Data ini juga digunakan untuk verifikasi dan triangulasi agar hasil penelitian lebih valid.

C. Indikator Efektivitas Cyber Threat Intelligence (CTI)

Penelitian ini menggunakan kerangka indikator untuk mengukur efektivitas implementasi *Cyber Threat Intelligence (CTI)* dalam konteks operasional sistem keamanan siber di BP Batam. Indikator yang digunakan disusun berdasarkan kajian literatur dan disesuaikan dengan karakteristik sektor pemerintahan, dengan tujuan memberikan arah yang sistematis dalam mengidentifikasi kontribusi *CTI* terhadap peningkatan kapabilitas keamanan informasi.

Gambar 2 berikut menyajikan representasi visual dari indikator efektivitas *CTI* yang menjadi dasar analisis penelitian ini.



Gambar 2. Visualisasi lima indikator efektivitas *CTI* yang digunakan dalam penelitian ini berdasarkan adaptasi dari Smallman (2024).

Indikator efektivitas dalam penelitian ini mencakup lima aspek utama yang dinilai relevan dan mewakili fungsi kunci dari sistem *CTI* berdasarkan adaptasi dari Smallman (2024) [3], yaitu kemampuan dalam mendeteksi dan merespons ancaman, dukungan terhadap pengelolaan risiko keamanan, kontribusi terhadap aktivitas *threat hunting*, potensi integrasi dengan sistem keamanan yang telah ada, serta relevansi dan akurasi data intelijen ancaman yang disediakan. Seluruh indikator ini menjadi dasar dalam penyusunan instrumen wawancara, reduksi data, analisis tematik, serta dalam interpretasi hasil temuan kualitatif.

Dengan pendekatan ini, indikator berfungsi tidak hanya sebagai landasan konseptual, tetapi juga sebagai instrumen analisis empiris untuk menilai sejauh mana penerapan CTI berkontribusi secara nyata terhadap sistem keamanan siber pada instansi pemerintahan yang menjadi objek penelitian.

D. Deskripsi Sistem dan Arsitektur OpenCTI

Penelitian ini menggunakan OpenCTI sebagai sistem utama, yakni sebuah *platform* intelijen ancaman siber berbasis *open-source* yang dirancang untuk mengelola, mengkategorikan, memvisualisasikan, dan membagikan informasi ancaman secara terstruktur dan relasional [10]. *OpenCTI* dikembangkan oleh Luatix dan dibangun untuk mendukung interoperabilitas data intelijen berdasarkan standar seperti *STIX 2.1* dan *TAXII 2.1.*

OpenCTI digunakan sebagai alat bantu untuk mengumpulkan dan menganalisis berbagai informasi ancaman, termasuk *indicator of compromise (IOC), threat actor*, *malware*, *tactics techniques and procedures (TTP),* serta berbagai entitas yang saling terhubung [17].

1) Komponen Utama Arsitektur OpenCTI : Pertama, *Frontend (Web Interface),* Komponen ini adalah antarmuka pengguna berbasis *ReactJS* yang memungkinkan visualisasi relasional antar entitas ancaman. Melalui tampilan grafis ini, pengguna dapat melihat korelasi antar IOC, *threat actor*, malware, dan teknik serangan dalam bentuk node-link diagram. Pengguna juga dapat melakukan pencarian, filter, dan tagging entitas tertentu berdasarkan sektor (pemerintah, militer, swasta, dll).

Kedua*, Backend (Core Engine),* Merupakan inti dari sistem yang bertanggung jawab untuk pengelolaan data, penyimpanan entitas, otorisasi pengguna, serta menjalankan logika bisnis. Backend dibangun menggunakan *GraphQL API* dan diatur melalui *database* berbasis *Elasticsearch* dan *Redis*. Sistem *backend* juga mencakup layanan scheduler untuk manajemen *job asynchronous.*

2) Connectors (Konektor): Connectors adalah skrip modular yang menghubungkan *OpenCTI* dengan berbagai sumber eksternal dan sistem lainnya. Connectors dapat dikategorikan menjadi dua jenis:

- *Import Connectors*: Mengambil data dari sumber eksternal (*CTI feeds*) dan memasukkannya ke *OpenCTI.*
- *Export Connectors*: Mengirimkan data dari *OpenCTI ke platform* lain (*SIEM, MISP*, dll).

Dalam penelitian ini, beberapa konektor yang digunakan adalah:

- *AlienVault (OTX Connector)*: Digunakan untuk mengimpor *indicator of compromise (IOC)* harian dari *Open Threat Exchange (OTX),* yaitu komunitas berbagi

e-ISSN: 2548-6861

ancaman global yang menyediakan feed terbuka dan relevan.

- *MISP (Malware Information Sharing Platform)*: Berfungsi sebagai integrasi dengan platform kolaboratif berbasis komunitas yang memungkinkan pertukaran informasi ancaman, seperti atribut *malware,* kampanye serangan, dan teknik eksploitasi. *Sharing Platform*
- *MalwareBazaar:* Konektor ini digunakan untuk menarik data *file hash*, keluarga *malware*, serta sampel berbahaya dari repositori *open-source* yang dikelola oleh komunitas *abuse.ch,* sehingga memperkaya konteks analisis malware di lingkungan *OpenCTI.*

3) Alur Kerja Sistem : Berikut ini adalah alur proses operasional *OpenCTI* di BP Batam:

- Data *IOC* ditarik secara otomatis melalui konektor dari berbagai feed harian berbasis *JSON* atau *STIX2*.
- *IOC* yang masuk divalidasi oleh sistem backend dan diindeks dalam *database OpenCTI.*
- *IOC* dan entitas lain yang relevan difilter berdasarkan sektor pemerintahan melalui fitur tagging dan filter.
- Informasi ancaman divisualisasikan di dashboard dan dapat diakses tim keamanan secara real-time.
- *IOC* dari *OpenCTI* dikorelasikan secara manual dengan log dari *firewall* dan *IDS* internal menggunakan analisis investigatif berbasis waktu dan sumber ancaman.
- Hasil investigasi digunakan untuk menyusun tindakan mitigasi, pemblokiran *IP/domain*, dan pelaporan ke tim keamanan internal.

4) Infrastruktur Sistem: Sistem *OpenCTI* dijalankan menggunakan *Docker Compose*, yang mencakup container untuk:

- *connector* (berbagai konektor)
- *elasticsearch (search engine)*
- *minio* (penyimpanan berkas)
- *redis (message broker)*

Sistem di-*deploy* di server lokal BP Batam menggunakan spesifikasi minimum:

- *Ubuntu Server 22.04 LTS*
- *8 vCPU, 16 GB RAM*
- Penyimpanan *SSD 500 GB*
- Akses terbatas melalui *VPN* internal

5) Keunikan Implementasi di BP Batam: Beberapa penyesuaian khusus yang dilakukan dalam implementasi *OpenCTI* ini antara lain:

- Pengembangan *dashboard* sektoral yang hanya menampilkan ancaman terhadap entitas pemerintah.
- Tidak dilakukan integrasi otomatis dengan *SIEM*, namun output *IOC* digunakan sebagai referensi untuk investigasi insiden secara manual.
- Semua data yang relevan dianalisis dan dilaporkan kepada tim keamanan internal secara berkala.

6) Metode Implementasi Sistem OpenCTI:

Penerapan *platform Cyber Threat Intelligence* (*CTI*) dalam penelitian ini dilakukan dengan menggunakan *OpenCTI*, sebuah sistem open-*source* yang dirancang untuk memfasilitasi pengumpulan, pengelolaan, dan visualisasi informasi ancaman secara terstruktur. Proses implementasi dilakukan secara bertahap dengan tujuan menyesuaikan lingkungan sistem terhadap kebutuhan instansi sektor pemerintahan, khususnya BP Batam.

Gambar 3 berikut memperlihatkan alur pengerjaan sistem *OpenCTI* yang digunakan dalam penelitian ini, mulai dari tahapan persiapan hingga korelasi *IOC* terhadap data keamanan internal.

Gambar 3. Alur Pengerjaan Sistem

Bagian ini menjelaskan sistem yang digunakan dalam penelitian, arsitektur teknis *OpenCTI*, serta bagaimana proses implementasi dan pemanfaatannya dilakukan di lingkungan BP Batam. Penjabaran dilakukan melalui lima aspek teknis berikut:

6) 1 Persiapan Lingkungan

Tahapan awal dimulai dengan menyiapkan server lokal yang digunakan sebagai lingkungan pengujian sistem. Sistem operasi yang digunakan adalah *Ubuntu Server* 22.04 LTS, dengan spesifikasi minimal: *8 vCPU, 16 GB RAM*, dan *500 GB SSD*. Untuk mempermudah manajemen layanan dan dependensi sistem, platform *OpenCTI* dijalankan menggunakan *Docker Compose*. Seluruh komponen inti seperti *elasticsearch*, *minio*, redis, dan *rabbitmq* dijalankan dalam *container* terpisah.

6) 2 Kloning dan Instalasi OpenCTI

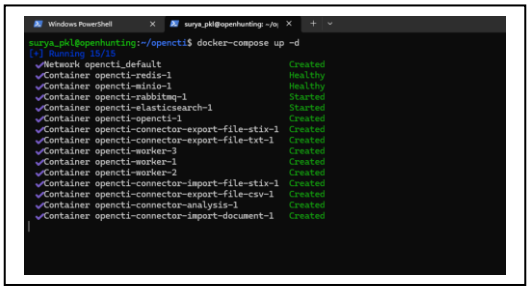
BProses instalasi dilakukan dengan mengkloning repositori resmi OpenCTI dari GitHub:

```
git clone https://github.com/OpenCTI-Platform/docker.git
```

Setelah itu, peneliti menyesuaikan file konfigurasi *.env* dan *docker-compose.yml* sesuai dengan spesifikasi sistem. Variabel yang diatur mencakup port akses *web, token API*, serta jalur data penyimpanan. Proses pengaktifan sistem dilakukan dengan menjalankan perintah:

```
docker-compose up -d
```

Tahap ini menghasilkan antarmuka web *OpenCTI* yang siap diakses melalui *browser* lokal dengan *URL* dan port yang telah ditentukan.



Gambar 4. Installasi OpenCTI

6) 3 Konfigurasi Konektor Eksternal *Threat Intelligence*

Setelah *platform* utama berjalan, tahapan berikutnya adalah mengaktifkan konektor untuk menarik *indicator of compromise* (*IOC*) dari berbagai sumber intelijen terbuka. Berikut konfigurasi konektor *AlienVault*, *MISP* dan *MalwareBazaar* di dalam container ditunjukkan pada potongan berikut:

Connector-Alienvault:

```
connector-alienvault:
  image: opencti/connector-alienvault:6.4.8
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    -
CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID
}
    - CONNECTOR_NAME=AlienVault
    - CONNECTOR_SCOPE=alienvault
    - CONNECTOR_LOG_LEVEL=error
    - CONNECTOR_DURATION_PERIOD=PT30M
 ALIENVAULT_BASE_URL=https://otx.alienvault.com
ALIENVAULT_API_KEY=1458f09483814497ad517546531498d8
0530f79927ff5e1000224b887cde6d
```

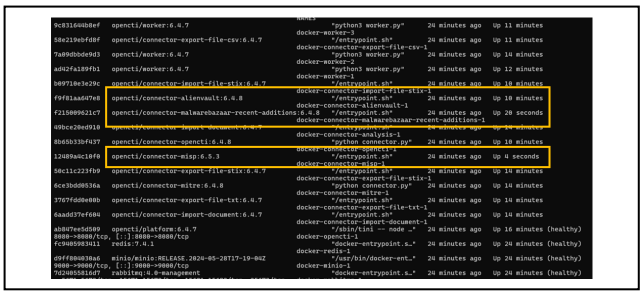
Connector-MISP:

```
connector-misp:
  image: opencti/connector-misp:6.5.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=26a4913d-164f-4b83-89ba-
5ed5f56bb8a6
    - CONNECTOR_ID=1487baed-f145-4236-afd8-c3e52ad5dbaf
    - CONNECTOR_NAME=MISP
    - CONNECTOR_SCOPE=misp
    - CONNECTOR_LOG_LEVEL=error
    - CONNECTOR_EXPOSE_METRICS=false
    - MISP_URL=https://192.168.206.131
```

Connector-Malwarebazaar:

```
connector-malwarebazaar-recent-additions:
  image: opencti/connector-malwarebazaar-recent-additions:6.4.8
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID
}
    - "CONNECTOR_NAME=MalwareBazaar Recent Additions"
    - CONNECTOR_LOG_LEVEL=error
```

Masing-masing konektor dikonfigurasi melalui file config.yml yang berisi parameter seperti *API key, URL endpoint, interval* sinkronisasi, serta pengaturan kategorisasi entitas. Setelah dijalankan, konektor bekerja secara mandiri untuk mengambil data *IOC* terbaru, yang kemudian dikirim ke sistem *backend OpenCTI* melalui *API* internal.



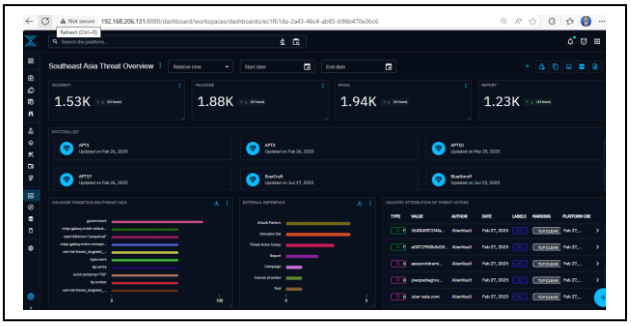
Gambar 5. Konektor Eksternal aktif

Gambar 5 berikut menunjukkan tampilan konektor eksternal yang telah berhasil dijalankan dan berada dalam status aktif (*running*) di lingkungan *Docker*. Aktivitas pengambilan data dapat dipantau melalui *log* konektor, yang mencatat waktu sinkronisasi, jumlah entitas yang berhasil diimpor, dan status masing-masing proses.

6) 4 Pengembangan *Dashboard* Sektoral

Dalam antarmuka *web OpenCTI*, peneliti mengembangkan dashboard yang difokuskan pada sektor pemerintahan. Ini dilakukan dengan mengatur *tag*, *filter*, dan *custom view* agar hanya menampilkan entitas ancaman yang relevan dengan domain publik. Visualisasi ini mempermudah tim keamanan dalam memantau ancaman yang spesifik terhadap instansi pemerintahan.

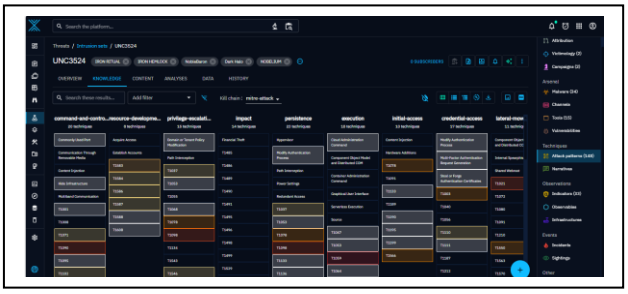
e-ISSN: 2548-6861



Gambar 6. *Dashboard Costum*

6) 5 Korelasi *IOC* dengan Data Internal

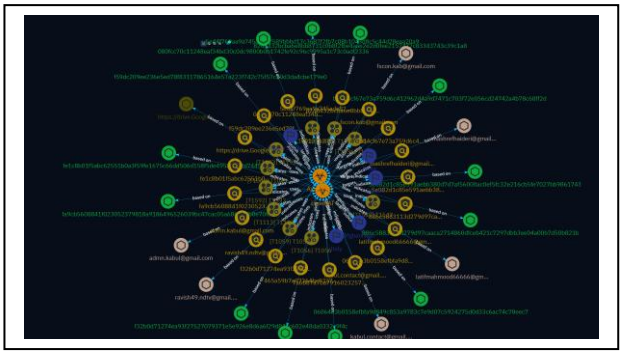
IOC yang berhasil ditarik dari berbagai sumber melalui konektor *OpenCTI* kemudian dikorelasikan secara manual dengan data log dari sistem internal, seperti *firewall, IDS/IPS*, dan sistem *email* organisasi. Proses korelasi dilakukan dengan mencocokkan entitas *IOC (IP address, domain, file hash,* dan *email*) terhadap aktivitas jaringan yang tercatat di *log* keamanan BP Batam.



Gambar 7. MITRE ATT&CK Matrix View

Gambar 7 memperlihatkan visualisasi teknik serangan dari intrusion set UNC3524, yang ditampilkan dalam format *MITRE ATT&CK matrix* di *dashboard OpenCTI*. Visualisasi ini membantu tim dalam mengidentifikasi taktik dan teknik yang digunakan oleh aktor ancaman serta relevansinya dengan *IOC* yang terdeteksi.

Sementara itu, Gambar 8 menunjukkan hubungan antara berbagai entitas *IOC* termasuk alamat *email*, *hash file*, dan domain yang terhubung dalam satu kampanye serangan. Korelasi semacam ini digunakan sebagai dasar analisis dan pelaporan insiden kepada tim keamanan internal.



Gambar 8. *Entity Relationship Graph*

E. Teknik Analisis Data

Penelitian ini menganalisis data menggunakan pendekatan tematik melalui penerapan model analisis kualitatif yang mencakup tujuh tahapan utama: wawancara, transkripsi, reduksi data, pemberian kode (koding), penyusunan matriks tematik, visualisasi data, hingga penyusunan narasi dan penarikan simpulan. Alur ini digunakan untuk memastikan bahwa proses analisis berlangsung secara sistematis, transparan, dan mampu menghasilkan interpretasi yang bermakna.

Alur keseluruhan teknik analisis data yang digunakan dalam penelitian ini ditunjukkan pada Gambar 8. Diagram ini menggambarkan urutan proses mulai dari pengumpulan data melalui wawancara hingga tahap penyusunan narasi dan penarikan simpulan tematik.

Gambar 9. Alur analisis data tematik dalam penelitian kualitatif fenomenologi.

Tahapan tersebut dilakukan sebagai berikut:

1) Wawancara: Proses analisis dimulai dari pengumpulan data melalui wawancara semi-terstruktur terhadap tiga informan utama di BP Batam. Wawancara difokuskan pada lima indikator efektivitas *CTI*, dengan pendekatan terbuka agar informan dapat menjelaskan pengalaman dan pandangannya secara luas terkait implementasi *OpenCTI* dan sistem keamanan internal.

2) Transkripsi: Seluruh hasil wawancara direkam dan kemudian ditranskripsikan secara verbatim untuk menjaga keaslian informasi. Transkrip menjadi dokumen dasar yang digunakan dalam proses reduksi dan koding.

3) Reduksi Data: Data yang telah ditranskrip kemudian disaring melalui proses reduksi, yaitu memilih bagian-bagian yang relevan dengan indikator penelitian. Kutipan yang tidak terkait langsung dengan tema efektivitas *CTI*, konteks sistem, atau pengalaman teknis tidak disertakan dalam tahap selanjutnya.

4) Pemberian Kode (koding): Proses pemberian kode dilakukan setelah data hasil wawancara direduksi dan difokuskan pada kutipan yang relevan. Setiap kutipan yang bermakna diberi label atau kode tematik untuk mempermudah pengelompokan data berdasarkan pola-pola yang muncul dari pernyataan narasumber.

Koding dilakukan secara manual dan induktif, artinya kode tidak ditentukan di awal, melainkan dikembangkan seiring pembacaan dan pemahaman terhadap isi data. Kode diberikan berdasarkan kata kunci, maksud ucapan, dan konteks penggunaan *CTI* yang muncul dalam wawancara.

5) Penyusunan Matriks Tematik: Setelah koding selesai, data yang telah diberi kode disusun ke dalam matriks tematik. Matriks ini berfungsi sebagai alat bantu untuk mengorganisir dan mengklasifikasi data secara terstruktur berdasarkan hubungan antara indikator penelitian, tema yang muncul, dan identitas narasumber. Penyusunan matriks tematik memungkinkan peneliti untuk mengidentifikasi distribusi data, kesamaan pola, dan perbedaan pandangan antar informan secara lebih jelas.

Matriks tematik juga menjadi landasan dalam proses analisis lanjutan dan menjadi penghubung antara data mentah dan narasi hasil penelitian.

6) Visualisasi Jaringan Tematik: Tahap visualisasi dilakukan untuk memetakan relasi antara indikator, tema/kode, dan hasil temuan secara konseptual dalam bentuk jaringan tematik. Visualisasi ini dibuat dalam format diagram yang menggambarkan keterkaitan antar elemen, dengan tujuan untuk memperjelas alur tematik yang ditemukan dari data kualitatif.

Visualisasi jaringan tematik berperan sebagai alat interpretatif yang memperkuat narasi penelitian dan membantu menunjukkan struktur logis dari hasil analisis. Dengan representasi visual ini, keterhubungan antara kategori yang dihasilkan melalui koding dapat digambarkan secara lebih intuitif dan mudah dipahami dalam konteks keseluruhan penelitian.

7) Narasi dan Simpulan Awal: Setelah seluruh proses analisis selesai, peneliti menyusun narasi deskriptif untuk menjelaskan kontribusi *Cyber Threat Intelligence* (CTI) pada masing-masing indikator efektivitas. Narasi ini dibangun berdasarkan hasil pengelompokan data tematik, yang kemudian diinterpretasikan dengan mengaitkannya pada kerangka teori dan konteks operasional di lapangan.

Simpulan awal ditarik dari konsistensi temuan antar narasumber, keterhubungan antar tema, serta bukti kontribusi nyata *CTI* dalam memperkuat sistem pertahanan siber di BP Batam.

Hasil dari tahap ini menjadi dasar utama dalam penyusunan uraian temuan lapangan yang dipaparkan secara sistematis pada bagian hasil dan pembahasan.

F. Validasi dan Kredibilitas Data

Validitas dan kredibilitas data dalam penelitian ini dijaga melalui beberapa strategi. Pertama, triangulasi dilakukan dengan menggabungkan data dari wawancara, observasi lapangan terhadap implementasi sistem *OpenCTI* dan dokumentasi teknis. Kedua, peneliti menerapkan *member checking* secara terbatas, yaitu dengan meminta konfirmasi dari informan terhadap interpretasi data yang diambil dari hasil wawancara yang signifikan.

Seluruh proses analisis juga dicatat secara sistematis melalui jejak audit (*audit trail*) guna menjamin konsistensi interpretasi. Selain itu, validitas diperkuat melalui diskusi dengan pembimbing untuk memastikan kesesuaian antara data lapangan dan kerangka analisis yang digunakan.

III. HASIL DAN PEMBAHASAN

Penelitian ini mengevaluasi efektivitas penerapan *Cyber Threat Intelligence* (*CTI*) melalui *platform OpenCTI* di lingkungan BP Batam. Analisis dilakukan berdasarkan lima indikator efektivitas yang dikembangkan berdasarkan sintesis dari studi Smallman, dengan pendekatan tematik berdasarkan hasil wawancara, observasi sistem, dan dokumentasi teknis.

A. Efektivitas Deteksi dan Respons terhadap Ancaman

Implementasi *OpenCTI* mempercepat proses deteksi dan respons terhadap ancaman. *IOC* yang diperoleh melalui konektor seperti *AlienVault* dan *MISP* membantu tim keamanan dalam memvalidasi insiden secara lebih terarah. Sebelumnya, analisis ancaman bergantung pada log manual dari *firewall* dan *IDS*, yang sering menimbulkan *false positive*.

Seorang analis menyatakan, “Sebelum ada *OpenCTI*, kami hanya mengandalkan notifikasi dari *firewall*. Sekarang kami bisa mencocokkan *IOC* langsung dengan sumbernya” (Informan A). Temuan ini sejalan dengan Smallman [3] yang menyebut bahwa *CTI* memberikan konteks yang memperkuat pengambilan keputusan insiden.

B. Dukungan terhadap Manajemen Risiko Keamanan

OpenCTI juga berperan dalam penguatan manajemen risiko. Informasi taktis seperti domain berbahaya, *TTP*, dan threat actor digunakan untuk menyusun kebijakan pemblokiran dan evaluasi risiko internal.

Kepala keamanan TI menyampaikan bahwa “dashboard *OpenCTI* mempermudah kami melihat siapa yang

e-ISSN: 2548-6861

mengancam sektor pemerintahan. Ini memperjelas prioritas mitigasi" (Informan B). Dukungan ini sesuai dengan penelitian Schlette et al. [4] yang menekankan pentingnya *CTI* dalam pengambilan keputusan berbasis risiko.

C. Peningkatan Aktivitas Threat Hunting

CTI juga memfasilitasi pendekatan threat hunting secara aktif. Tim keamanan melakukan pencocokan *IOC* ke dalam log sistem untuk mencari aktivitas mencurigakan secara manual, namun lebih terfokus dan terarah.

Seorang informan menyebut, "Kami tidak hanya menunggu serangan. Sekarang kami proaktif mencari pola *IOC* dari *OpenCTI* yang cocok dengan aktivitas di jaringan internal" (Informan C). Hal ini mencerminkan transisi dari deteksi pasif ke pendekatan berbasis hunting yang lebih dinamis, sebagaimana didukung oleh Gao et al. [5].

D. Integrasi dengan Sistem Keamanan yang Ada

Meskipun integrasi otomatis belum dilakukan, *OpenCTI* digunakan untuk validasi hasil dari sistem seperti *SIEM*, *IDS*, dan *firewall*. *IOC* dari *OpenCTI* dipakai sebagai pembanding *log*, dan entitas seperti *IP*, *domain*, serta *hash malware* dikonfirmasi secara manual.

Menurut salah satu informan, "Kami belum bisa sambungkan langsung dengan *SIEM*, tapi kami gunakan *IOC OpenCTI* sebagai bahan investigasi tambahan" (Informan A). Hal ini menunjukkan adanya pemanfaatan tak langsung, namun tetap memperkaya sistem yang ada.

E. Relevansi dan Akurasi Data Intelijen

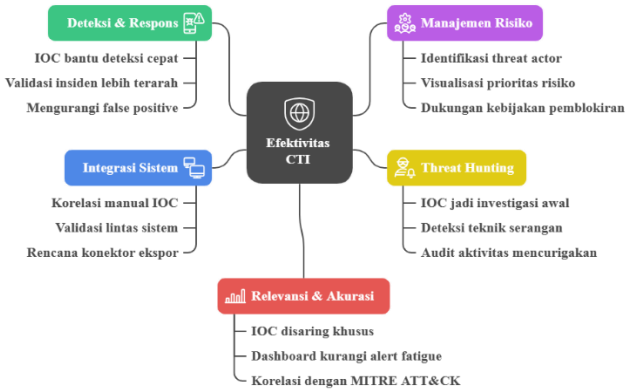
Penyesuaian *dashboard* sektoral memperkuat relevansi data intelijen. Ancaman yang muncul di dashboard telah difilter khusus untuk sektor pemerintahan, sehingga meminimalkan *alert fatigue* dan meningkatkan efisiensi analisis.

Kepala keamanan menyatakan, "Kami hanya lihat yang relevan dengan sektor pemerintah. Itu menghemat waktu dan membuat analisis kami lebih fokus" (Informan B). Studi Kayode-Ajala [7] menunjukkan bahwa kustomisasi sektoral meningkatkan efektivitas adopsi *CTI* dalam organisasi.

F. Visualisasi Temuan Tematik

Visualisasi temuan tematik bertujuan untuk menggambarkan hubungan antara indikator efektivitas *Cyber Threat Intelligence (CTI)* dengan hasil-hasil temuan lapangan yang diperoleh melalui proses koding dan analisis tematik. Visualisasi ini disusun dalam bentuk jaringan diagram tematik yang merepresentasikan kontribusi implementasi OpenCTI terhadap lima indikator utama, yaitu *Deteksi & Respons*, *Manajemen Risiko*, *Threat Hunting*, *Integrasi Sistem*, dan *Relevansi & Akurasi*.

Gambar 10 menyajikan jaringan hubungan antar elemen, di mana setiap panah mengindikasikan kontribusi temuan terhadap indikator yang bersangkutan.



Gambar 10. Visualisasi Jaringan Tematik antara Indikator Efektivitas CTI dan Temuan Lapangan.

Untuk memudahkan pemahaman terhadap visualisasi tersebut, Tabel 1 di bawah ini memberikan penjabaran naratif yang menjelaskan makna setiap hubungan pada diagram jaringan tematik.

Tabel 1. Penjelasan Visualisasi Jaringan Tematik

Indikator	Temuan Tematik	Penjelasan Hubungan
Deteksi & Respons	IOC bantu deteksi cepat	IOC dari konektor seperti *AlienVault & MISP* digunakan untuk mempercepat deteksi insiden yang relevan di lingkungan BP Batam.
	Validasi insiden lebih terarah	IOC digunakan sebagai acuan utama dalam proses validasi insiden, sehingga tidak hanya bergantung pada notifikasi dari sistem *IDS/Firewall.*
	Mengurangi *false positive*	Korelasi IOC dengan log internal membantu menyaring alarm palsu yang umum terjadi pada sistem deteksi konvensional.
Manajemen Risiko	Identifikasi *threat actor*	*CTI* memungkinkan identifikasi aktor ancaman yang relevan dengan sektor publik, membantu tim menyusun strategi mitigasi.
	Visualisasi prioritas risiko	*Dashboard* sektoral menyajikan ancaman berdasarkan sektor, sehingga mempermudah

		penentuan prioritas penanganan.
	Dukungan kebijakan pemblokiran	*IOC* yang terverifikasi mendukung proses pengambilan keputusan untuk pemblokiran *IP* atau domain yang berisiko.
Threat Hunting	*IOC* jadi investigasi awal	*IOC* digunakan sebagai titik awal investigasi untuk menelusuri jejak ancaman pada log sistem secara manual.
	Deteksi teknik serangan	*IOC* dihubungkan dengan teknik serangan (*TTP*) seperti *abuse PowerShell* untuk menemukan pola serangan tersembunyi.
	Audit aktivitas mencurigakan	IOC memperkuat audit terhadap aktivitas internal seperti command line atau PowerShell log yang mencurigakan.
Integrasi Sistem	Korelasi manual *IOC*	*IOC* dari *OpenCTI* digunakan untuk validasi manual terhadap log *SIEM*, *firewall*, dan *IDS* dalam investigasi insiden.
	Validasi lintas sistem	Data dari *CTI* memperkaya hasil analisis dari sistem lain, memungkinkan verifikasi silang antar *platform* keamanan.
	Rencana konektor ekspor	Meski belum otomatis, ada inisiatif mengembangkan konektor untuk integrasi langsung ke sistem seperti *SIEM*.
Relevansi & Akurasi	*IOC* disaring khusus	Ancaman disaring hanya yang berkaitan dengan sektor pemerintahan untuk menjaga relevansi dan efisiensi analisis.
	Dashboard kurangi *alert fatigue*	Visualisasi ancaman yang telah difilter mengurangi jumlah notifikasi tidak penting, meningkatkan fokus dan akurasi analisis.
	Korelasi dengan MITRE ATT&CK	IOC dan entitas lain dikaitkan dengan taktik dan teknik serangan dari MITRE ATT&CK untuk memperkuat konteks ancaman yang dianalisis.

IV. KESIMPULAN

Penelitian ini bertujuan untuk menganalisis efektivitas penerapan *Cyber Threat Intelligence* (*CTI*) melalui *platform OpenCTI* dalam meningkatkan ketahanan keamanan siber di lingkungan BP Batam. Hasil penelitian menunjukkan bahwa *OpenCTI* berkontribusi nyata terhadap lima aspek utama: peningkatan efektivitas deteksi dan respons, dukungan terhadap manajemen risiko keamanan, penguatan aktivitas *threat hunting*, integrasi fungsional dengan sistem keamanan yang telah ada, serta peningkatan relevansi dan akurasi data intelijen. Implementasi *CTI* mendorong perubahan pendekatan keamanan dari reaktif menjadi proaktif, dengan pemanfaatan *IOC* dan *threat actor* yang sesuai dengan kebutuhan sektor pemerintahan. Meskipun integrasi sistem belum sepenuhnya otomatis, *CTI* telah digunakan secara strategis dalam investigasi ancaman dan penyusunan mitigasi. Penelitian ini merekomendasikan agar BP Batam terus mengembangkan integrasi teknis *OpenCTI* dengan sistem keamanan lainnya secara otomatis dan memperluas cakupan *dashboard* sektoral untuk meningkatkan efisiensi analisis ancaman. Penelitian selanjutnya dapat dilakukan dengan pendekatan perbandingan pada instansi pemerintah lain atau dengan penguatan evaluasi berbasis metrik kuantitatif.

UCAPAN TERIMA KASIH

Penulis mengucapkan apresiasi kepada Badan Pengusahaan Batam (BP Batam) atas dukungan dan fasilitas yang diberikan selama proses pelaksanaan penelitian ini, serta menyediakan data dan akses sistem yang diperlukan guna menunjang proses observasi dan analisis. Tanpa dukungan tersebut, penelitian ini tidak dapat dilaksanakan secara optimal.

DAFTAR PUSTAKA

[1] Id-SIRTII /CC, “Lanskap Keamanan Siber Indonesia,” *Id-SIRTII /CC*, no. 70, pp. 1–107, 2024.

[2] Sofyan, Ed., *Cost-of-Doing-Business-in-Batam-2023.pdf*. Batam: Promotion BP Batam, 2023.

[3] J. Smallman, “The Effectiveness of Cyber Threat Intelligence in Improving Security Operations,” *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*, vol. 5, no. 1, pp. 189–209, 2024, doi: 10.60087/jaigs.v5i1.193.

[4] D. Schlette, M. Caselli, and G. Pernul, “A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2525–2556, 2021, doi: 10.1109/COMST.2021.3117338.

[5] P. Gao *et al.*, "Enabling efficient cyber threat hunting with cyber threat intelligence," *Proc Int Conf Data Eng*, vol. 2021-April, pp. 193–204, 2021, doi: 10.1109/ICDE51399.2021.00024.

[6] N. Sun *et al.*, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 3, pp. 1748–1774, 2023, doi: 10.1109/COMST.2023.3273282.

[7] O. Kayode-Ajala, "Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption," *Applied Research of Artificial Intelligence and Cloud Computing*, vol. 6, no. 1, pp. 1–21, 2023, [Online]. Available: https://researchberg.com/index.php/araic/article/view/159

[8] V. Jesus, B. Bains, and V. Chang, "Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence," *IEEE Trans Eng Manag*, vol. 71, pp. 6854–6873, 2024, doi: 10.1109/TEM.2023.3279274.

[9] P. Gao, X. Liu, E. Choi, S. Ma, X. Yang, and D. Song, "*ThreatKG:* An AI-Powered System for Automated Open-Source Cyber Threat Intelligence Gathering and Management," in *Proceedings of the 1st ACM Workshop on Large AI Systems and Models with Privacy and Safety Analysis*, New York, NY, USA: ACM, Nov. 2023, pp. 1–12. doi: 10.1145/3689217.3690613.

[10] S. Ruohonen, A. Kirichenko, D. Komashinskiy, and M. Pogosova, "Instrumenting OpenCTI with a Capability for Attack Attribution Support," *Forensic Sciences*, vol. 4, no. 1, pp. 12–23, 2024, doi: 10.3390/forensicsci4010002.

[11] A. Nasir, K. Shah, R. A. Sirodj, and M. W. Afgani, "Pendekatan Fenomenologi Dalam Penelitian Kualitatif," vol. 3, pp. 4445–4451, 2023.

[12] O. Hasbiansyah, "Pendekatan Fenomenologi : Pengantar Praktik Penelitian dalam Ilmu Sosial dan Komunikasi," no. 56, pp. 163–180, 2005.

[13] Y. Yusanto, "Ragam Pendekatan Penelitian Kualitatif," vol. 1, no. 1, pp. 1–13, 2019.

[14] P. Muhammad *et al.*, "Metodologi Penelitian Kualitatif," 2023. [Online]. Available: https://www.researchgate.net/publication/370561417

[15] C. Moustakas, "Phenomenological Research methods."

[16] "Qualitative inquiry & research design. design _ Choosing among five approaches. (1)".

[17] M. Opencti, S. Sumber, and I. Mandiri, "Strategi Alternatif : OpenCTI Tanpa Integrasi Langsung dengan Sistem Pemantauan".