Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 7, No. 09, September 2022

COLLABORATIVE CYBER THREAT INTELLIGENCE: MEMPERKUAT KEAMANAN SIBER NASIONAL MELALUI KERJASAMA CSIRT

Farlin Hottua Sigiro[1*], Arthur Josias Simon Runturambi[2], Bondan Widiawan[3]
[1*,2,3]Sekolah Kajian Stratejik dan Global, Universitas Indonesia, Indonesia
Email: [1*]farlin.hottua@ui.ac.id, [2]simonrbi@yahoo.com, [3]bondan.w@ui.ac.id

Abstrak

Sistem keamanan siber dalam beberapa tahun terakhir berkembang dan terlembaga, hal ini dikarenakan faktor keamanan siber telah menjadi perhatian penting, terutama pemerintah Indonesia. Pemerintah melalui BSSN telah banyak me-*launching* CSIRT *(Computer Security Incident Response Team)*. CSIRT merupakan Tim Tanggap Insiden yang memberikan layanan untuk melindungi sistem atas insiden siber. Meskipun demikian, fenomena insiden siber yang menimpa sektor pemerintah tetap masif. Di sisi lain, lanskap keamanan siber dalam tiga tahun terakhir menunjukkan bahwa kemampuan ancaman siber meningkat signifikan, dan jumlahnya semakin banyak, puluhan varian *malware* muncul setiap bulan. Oleh karena itu, lembaga dan organisasi tidak cukup dengan melakukan pemantauan dan respon insiden yang bersifat reaktif, namun harus mengubah strategi dengan menggabungkan langkah-langkah keamanan preventif dengan intelijen ancaman. Pengembangan kemampuan Intelijen Ancaman Siber (CTI) dinilai sangat efektif untuk meningkatkan postur keamanan siber. Saat ini program CTI ada di BSSN. Namun, distribusi informasi masih bersifat satu arah, dari BSSN ke CSIRT lembaga. Penelitian ini menggunakan pendekatan kualitatif dengan teknik menggunakan studi kajian pustaka dari penelitian sebelumnya observasi. Hasil penelitian ini menunjukkan terdapat trend ancaman siber semakin tinggi dalam dua tahun terakhir. Beberapa insiden mengalami ekskalasi ancaman pada informasi vital nasional. Oleh karena itu intelijen ancaman siber sektor pemerintah harus dikerjakan bersama-sama oleh komunitas CSIRT. Di akhir, penelitian ini mengusulkan model *collaborative sharing* CTI yang melibatkan seluruh CSIRT pada masing-masing sektor untuk meningkatkan keamanan siber nasional.

Kata kunci: Lanskap Ancaman Siber, CTI, *Collaborative Sharing*, Keamanan Siber Nasional.

How to cite:	Farlin Hottua Sigiro, Arthur Josias Simon Runturambi, Bondan Widiawan (2023) Collaborative Sharing Intelijen Ancaman Pada Komunitas Csirt Dalam Memperkuat Keamanan Siber Nasional, *(7) 09,* https://doi.org/10.36418/syntax-literate.v7i9.14245
E-ISSN:	2548-1398
Published by:	Ridwan Institute

Abstract

In recent years, the cyber security system has developed and become institutionalized, this is because cyber security has become an important concern, especially for the Indonesian government. The government through BSSN has launched many CSIRT (Computer Security Incident Response Team). CSIRT is an Incident Response Team that provides services to protect systems for cyber incidents. Despite this, the phenomenon of cyber incidents affecting the government sector remains massive. On the other hand, the cyber security landscape in the last three years shows that cyber threat capabilities have increased significantly, and their number is increasing, with dozens of malware variants appearing every month. Therefore, it is not enough for institutions and organizations to carry out reactive monitoring and incident response, but must change their strategy by combining preventive security measures with threat intelligence. The development of Cyber Threat Intelligence (CTI) capabilities is considered very effective in improving cyber security posture. Currently the CTI program is available at BSSN. However, information distribution is still one-way, from BSSN to CSIRT institutions. This research adopts a qualitative approach with techniques using literature review studies from previous observational research. The results of this research show that there is a trend of increasingly high cyber threats in the last two years. Several incidents escalated threats to vital national information. Therefore, cyber threat intelligence in the government sector must be carried out jointly by the community. At the end, this research proposes a collaborative sharing CTI model that involves all CSIRTs in each sector to improve national cyber security.

Keywords: *cyber threat landscape, CTI, collaborative sharing, national cyber security.*

Pendahuluan

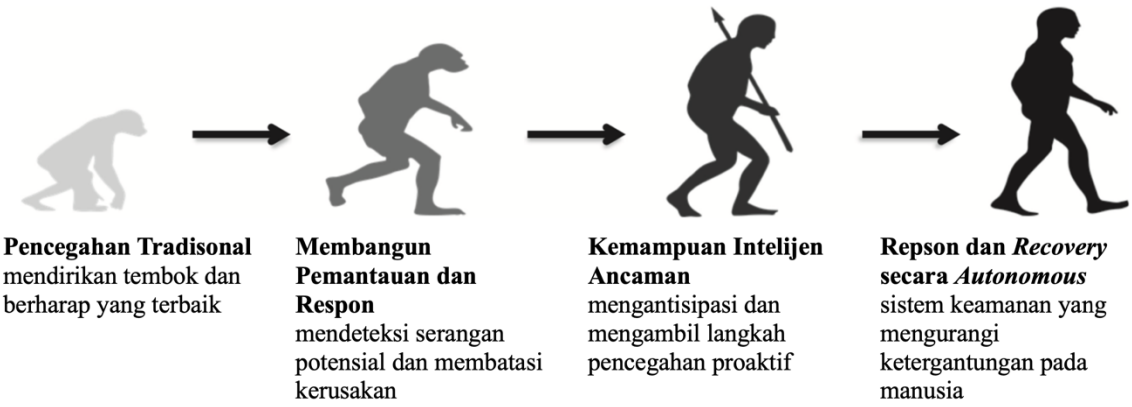
Saat ini perkembangan kemampuan ancaman siber telah meningkat signifikan (Fransen & Kerkdijk, 2017) dan dalam beberapa tahun terakhir lanskap ancaman siber berkembang sangat pesat dan telah menjadi canggih, terkoordinasi, dan dapat disesuaikan (Skopik, Settanni & Fiedler, 2017). Hal ini mengakibatkan dampak insiden siber menimpa berbagai sistem dan infrastruktur baik secara global (M-Trends, 2023) dan di dalam negeri (BSSN, 2023). Secara global telah terjadi peningkatan insiden siber yang menyerang berbagai sektor (Mandiant, 2023). Sementara di dalam negeri terjadi peningkatan insiden yang menimpa berbagai sektor yang didalamnya terdapat informasi kritis (Putra, 2022). Dalam dua tahun terakhir telah terjadi insiden siber yang sangat signifikan seperti kebocoran data peretasan website dalam bentuk phishing dan DDoS (BSSN, 2021; BSSN, 2023). Adapun serangan siber lainnya yang terjadi marak adalah penyebaran *malware* lewat file APK, perang informasi dalam bentuk penyebaran hoaks, peretasan website menjadi tampilan judi online (BSSN, 2023). Semua hal ini mengakibatkan transformasi digital yang sedang marak dilaksanakan secara global menghadapi ancaman dan ketidakpastian dalam ruang siber.

Dalam lanskap ancaman siber secara global, laporan Mandiant Special Report 2023, mencatat bahwa pada rentang tahun 2021 dan 2022 terjadi peningkatan insiden pencurian data, peningkatan jumlah Kelompok Ancaman (Multiple Threat Group), dan munculnya puluhan varian malware setiap bulannya. Sementara dalam laporan lanskap ancaman siber dalam negeri, sepanjang tahun 2022, berbagai jenis ancaman siber telah secara signifikan menargetkan ruang siber Indonesia. Insiden siber seperti kebocoran data breach dan darknet exposure. Berbagai jenis insiden yang menimpa, diantaranya: *malware, malicious activity, ransomware, web defacement, phishing*, kebocoran data, kerentanan, isu IPOLEKSOSBUDHANKAM, dan *advanced persistent threats*-APT (BSSN, 2023). Dan sepanjang tahun 2021, juga terjadi fenomena yang mirip. Laporan tersebut terdiri atas: *data breach, ransomware, profiling, web defacement, malicious activity, dark web enabled crime, compromised account*, dan *web phishing*. Atas kejadian tersebut telah dilakukan pendalaman investigasi pada puluhan sistem lembaga untuk mengungkap aktor pelaku (BSSN, 2022). Dalam laporan BSSN 2022, ditemukan lebih dari empat juta aktivitas APT di Indonesia.

Gambar 1. Lanskap ancaman siber
(sumber: ENISA Threat Landscape 2022 - Prime Threats)

Perkembangan kemampuan ancaman siber terdeteksi dengan semakin banyaknya varian malware dengan kemampuan unik (M-Trends, 2023). Kemudian, munculnya serangan siber dengan metode serangan tingkat tinggi seperti *Advanced Persistent Threat* (APT), yang sangat terorganisir dan kompleks, berpotensi menimbulkan konsekuensi serius, bahkan pada tingkat nasional (Pahi & Skopik, 2017). Perkembangan tersebut juga semakin mempersulit para analis keamanan siber untuk mengupayakan pertahanan siber. Kelompok ancaman siber seperti APT adalah risiko serius karena mereka bersifat adaptif dan inovatif, mengupayakan teknik terbaru dan segala upaya untuk melakukan penyerangan (Benson, 2022), spionase, pencurian data, dan perolehan akses ilegal. Kini, organisasi dan pemerintahan tidak hanya menghadapi jenis ancaman yang semakin canggih yang telah dijelaskan di atas, namun juga menghadapi para aktor penyerang yang juga semakin profesional dan terorganisir untuk melakukan penyerangan (Pahi & Skopik,

2017). Oleh karena itu, kemampuan daya tangkal dan respon insiden oleh para tim CSIRT *(Computer Security Incident Response Team)* semakin berat. Strategi lama seperti pemanfaatan sistem monitoring internal, analisis log dan trafik kurang mumpuni dan tidak relevan lagi untuk menghadapi perkembangan ancaman siber yang canggih.



Gambar 2. Evolusi strategi ketahanan siber
Sumber: diolah dari (Fransen & Kerkdijk, 2017)

Dalam menghadapinya, organisasi dan pemerintahan terpaksa harus melakukan perubahan strategi peningkatan keamanan siber, dari yang sebelumnya strategi reaktif dengan melakukan tindakan saat insiden sudah terjadi, menjadi strategi preventif dengan melakukan intelijen ancaman baik dari dalam sistem maupun dari luar serta harus proaktif untuk saling membantu membangun pertahanan siber. Melawan ancaman siber saat ini memerlukan tenaga kerja multidisipliner, setidaknya ada dalam bidang siber dan intelijen (Benson, 2022). Penerapan intelijen ancaman menjadi hal penting saat ini. Di Indonesia sendiri, penerapan CTI sudah diimplementasikan di beberapa perusahaan swasta, sementara di pemerintahan telah diinisiasi BSSN sejak tahun 2021 yang bertransformasi dari Pusat Operasi Keamanan Siber (BSSN, 2021). BSSN sejauh ini secara rutin mempublikasikan laporan-laporan seperti: kerentanan dan laporan anomali, *top malware, profiling threat actor, lesson learned,* dan informasi umum keamanan siber secara nasional maupun global. Namun, laporan tersebut belum berdampak maksimal karena sifatnya hanya publikasi dan rekomendasi, tidak ada dorongan atau kewajiban untuk melakukannya, selain itu dalam proses intelijen ancaman hanya dilaksanakan oleh BSSN dan sektor lain hanya terbatas sebagai penerima rekomendasi, hal ini akan berdampak pada kurangnya komitmen dan keterlibatan pelaksanaan. Oleh karena itu, strategi baru yakni proaktif dan preventif dapat memberi manfaat pada penguatan keamanan jika di dalamnya terjadi kolaborasi antar lembaga dalam menghadapi ancaman bersama (Leitner, Pahi & Skopik, 2017).

Sistem keamanan siber dalam beberapa tahun terakhir sudah berkembang dan terlembaga, hal ini dikarenakan faktor keamanan siber telah menjadi perhatian utama baik untuk pemerintah maupun swasta dalam menjalankan bisnis (Saeed et al., 2023). Dalam mengikuti perkembangan zaman, pemerintah Indonesia sangat antusias mewujudkan ketahanan siber nasional lewat pembentukan CSIRT, namun saat ini masih berfokus pada

sektor pemerintah. Agenda utama CSIRT masih dalam membangun kerja sama, *capacity building*, dan *sharing knowledge* agar dapat memberi pelayanan sesuai pembentukan awal. Layanan CSIRT saat ini belum banyak berubah dari pertama dicanangkan, sementara fungsinya dapat dimaksimalkan melalui proses *threat hunting* untuk menghasilkan informasi intelijen ancaman (CTI) guna mendukung operasi keamanan siber atau *Security Operations Center* (SOC) yang lebih handal.

Namun bagaimanapun, dari sisi implementasi, program CTI masih menghadapi kendala baik dalam tataran teknis maupun manajemen, standar pertukaran yang cukup banyak mengakibatkan proses komunikasi menjadi kompleks (Liu et al., 2019), aspek legal yang belum pasti yang berdampak pada klasifikasi data maupun koordinasi dan kerja sama menjadi terhambat (Schroers & Clifford, 2017). Perbedaan standar mengakibatkan proses pertukaran menjadi sangat kompleks, hal ini mengakibatkan intelijen ancaman di suatu entitas tidak segera menjadi informasi untuk entitas lainnya untuk dioperasikan sehingga para aktor penyerang berpotensi lebih besar untuk melakukan serangan. Disisi lain, masih lebih banyak organisasi yang belum melakukan program intelijen siber. Permasalahan intelijen ancaman berikutnya adalah tidak adanya kerja sama dan koordinasi dalam menghadapi ancaman bersama. Biasanya para aktor penyerang akan selalu mempelajari kelemahan dan kerentanan suatu sistem. Aktor penyerang akan melakukan penyerangan ketika menemukan kerentanan dan kelemahan. Tantangan koordinasi, kerja sama dapat berjalan mulus jika aspek teknis dan aspek manajerial

Dalam penelitian ini, penulis mengusulkan implementasi program CTI secara kolaboratif antar lembaga dalam menghadapi ancaman. Usulan ini dapat dimanfaatkan oleh pemerintah untuk menyusun kebijakan dalam peningkatan keamanan siber nasional. Pertukaran informasi intelijen secara kolaboratif diharapkan mendorong koordinasi dan kerja sama yang lebih optimal antar lembaga meningkatkan keamanan siber nasional.

Metode Penelitian

Penelitian ini akan mengadopsi pendekatan kualitatif deskriptif. Pendekatan kualitatif yang berdasarkan data-data yang diperoleh dari laporan tahunan monitoring ancaman siber BSSN dalam 3 tahun terakhir, laporan intelijen ancaman siber Uni Eropa, Amerika Serikat, dan Global yang dikeluarkan oleh organisasi-organisasi dan perusahaan keamanan siber terkemuka maupun. Penulis juga mengkombinasikan dengan kajian pustaka baik dari jurnal terindeks, buku, *whitepaper*, dan sumber online terbuka.

Pemilihan pendekatan kualitatif dan analisis deskriptif dengan pertimbangan yang cermat karena sejalan dengan tujuan penelitian untuk memperoleh pemahaman yang mendalam dan deskriptif mengenai fenomena yang sedang diteliti. Pendekatan kualitatif deskriptif memiliki ciri khasnya sendiri. Pertama, pendekatan ini fokus pada pengumpulan dan analisis data yang bersifat kualitatif, seperti kata-kata dan teks, yang diperoleh dari partisipan atau subjek penelitian (Creswell, 2017). Jenis data ini memungkinkan peneliti untuk menjelaskan fenomena dengan detail dan mendalam serta menggambarkannya secara kontekstual.

Adapun tujuan penelitian ini adalah untuk mengetahui dan menganalisis trend perkembangan signifikan ancaman siber dan upaya pemerintah dalam menghadapinya, kemudian menganalisis pengembangan CTI, diakhir mengusulkan pertukaran informasi ancaman secara kolaboratif antar lembaga dalam meningkatkan keamanan siber nasional.

Hasil dan Pembahasan

Berbagai insiden siber dalam beberapa tahun terakhir telah mengakibatkan ancaman nyata yang dihadapi masyarakat saat ini. Seperti pada bulan Mei 2023 terjadi insiden yang mengejutkan yakni insiden siber pada Bank Syariah Indonesia (BSI). BSI menjadi target serangan *ransomware* yang mengakibatkan sistem lumpuh selama empat hari (Republika, 2023). Di sektor yang sama, pada tahun 2021, Bank Jatim dan BRI Life, yang merupakan anak perusahaan BRI di bidang asuransi, mengalami serangan siber dan dugaan kebocoran data pribadi nasabah di internet. Bahkan, pada awal tahun 2022, Bank Indonesia juga mengungkapkan bahwa mereka telah menjadi korban serangan *ransomware* (BBC News, 2023). Insiden lain juga terjadi pada sektor kesehatan. Dugaan kebocoran data BPJS Kesehatan yang diperkirakan dapat menimbulkan kerugian besar. Menurut laporan tim *Cyber Security Independent Resilience Team* (CSIRT), kerugian finansial akibat kebocoran 279 juta data peserta Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan mencapai Rp 600 triliun. Para ahli dalam bidang informasi dan teknologi berpendapat bahwa hal ini terjadi karena eksploitasi data kependudukan (Burhan, 2021). Selain sektor perbankan dan sektor kesehatan, masih banyak insiden yang terjadi pada sektor lainnya. Insiden-insiden ini menyadarkan kita bahwa krisis akibat dari serangan siber bisa datang tanpa diduga. Penting untuk kita semua agar selalu siap dan memiliki rencana untuk menghadapinya (Aruman, 2023).

Insiden-insiden siber yang semakin masif tidak dapat dipungkiri karena perkembangan teknologi informasi dan semakin bergantungnya banyak pekerjaan pada ruang siber. Dalam era *Society* 5.0, berbagai aktivitas manusia akan terkonsentrasi pada pusat-pusat manusia berbasis teknologi (Ardiansyah & Amalia, 2023). Hampir seluruh aktivitas manusia sudah terintegrasi ke dalam ruang siber. Mulai dari sistem pendidikan, perbankan, pemerintahan, swasta, dan sektor-sektor penting lainnya. Proses digitalisasi ini semakin menyeluruh dengan bantuan kecerdasan buatan yang semakin kompleks. Revolusi digital yang berlangsung saat ini tidak hanya menambah berbagai keuntungan namun sekaligus menambah ruang munculnya serangan siber. Evolusi integrasi ruang siber saat ini sangat berpotensi menimbulkan kejutan strategis dan krisis secara tiba-tiba (Barnea, 2020). Kejutan krisis yang kita alami saat ini merupakan insiden yang muncul ke permukaan. Sementara keberadaan ruang siber yang evolutif menyimpan banyak potensi kejutan-kejutan strategis lainnya ke depan. Perlu upaya untuk meningkatkan keamanan siber salah satunya dapat dicapai dengan adanya kolaborasi antara pemerintah dan pihak swasta (DPR RI, 2021).

A. Tren Insiden Global

Dalam skala global dari laporan Mandiant Special Report 2023, mencatat bahwa pada tahun 2022 insiden pencurian data mengalami peningkatan menjadi 40%

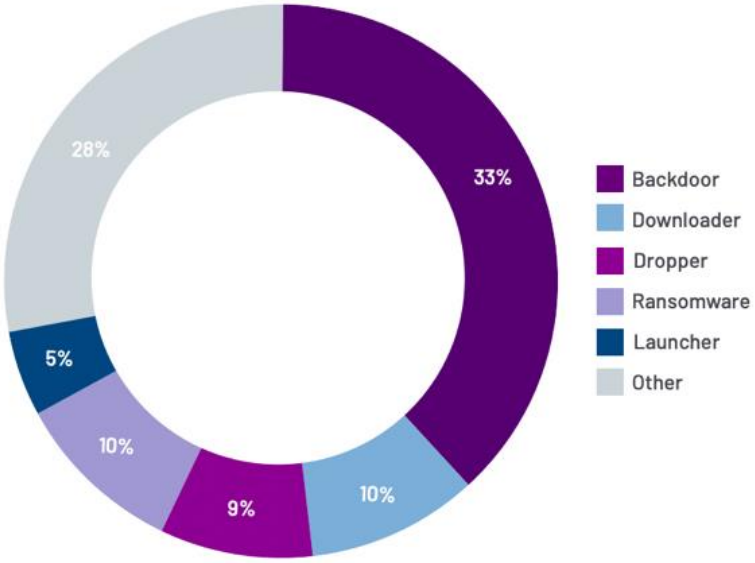
dari tahun sebelumnya 29%, teridentifikasi peningkatan Kelompok Ancaman (*Multiple Threat Group*) menjadi 27% dari tahun sebelumnya 25% dari total lebih dari 3500 grup. Investigasi terhadap *malware* sebanyak 588 *malware* baru dengan rata-rata 49 per bulan, dibandingkan dengan tahun 2021 yakni 45 per bulan.

Tabel 1
Sebaran Sektor Tertarget Global

No.	Sektor	Jumlah
1.	Pemerintahan	25%
2.	Business dan Profesional	14%
3.	Finansial	12%
4.	Teknologi Tinggi	9%
5.	Kesehatan	9%
6.	Ritel dan Jasa	6%
7.	Media dan Hiburan	5%
8.	Konstruksi	5%
9.	Telekomunikasi	4%
10.	Logistik dan Transportasi	3%
11.	Pendidikan	2%
12.	Perangkat	2%
13	Nonprofit	1%
14	Energi	1%

Sumber: Diolah dari M-Trends 2023

Para ahli mengamati bahwa terdapat 321 keluarga *malware* baru yang melakukan intrusi sepanjang tahun 2022, sejumlah 29% dari total *malware* yang terdeteksi. *Backdoor* masih menjadi elemen pokok yang digunakan sebanyak 33%, meski turun 7% dari tahun 2021, namun varian ini terdeteksi jauh lebih banyak dari varian lain. Berikutnya adalah varian *Downloader* (10%), *Ransomware* (10%), *Droppers* (9%), dan *Launcher* (5%) sebagai lima teratas (M-Trends, 2023).



Gambar 3. Investigas Varian Malware Berdasarkan Kategori
Sumber: M-Trends, 2023, Mandiant Special Report

Di kawasan Uni Eropa, European Union Agency for Cyber Security (ENISA) dalam laporan Threat Landscape 2022 mencatat bahwa ancaman-ancaman utama yang teridentifikasi ada delapan, diantaranya: *ransomware, malware, social engineering threats, threats against data, Denial of Service (DoS), internet threats, disinformation-misinformation,* dan *supply-chain attacks.* Adapun aktor-aktor dari ancaman tersebut dikategorikan menjadi empat, yakni: *state-sponsored actors, cybercrime actors, hacker-for-hire actors, hacktivists* (ETL, 2022). Sebagian besar insiden menyasar administrasi publik dan pemerintahan serta penyedia digital. Dalam laporan tahun 2016, ENISA juga mencatat bahwa telah terjadi perkembangan ancaman siber yang signifikan. Salah satunya adalah munculnya *"Cyber-crime-as-a-Service,"* di mana alat-alat disediakan secara mudah yang digunakan oleh penyerang tanpa kebutuhan teknis untuk mengembangkan alat mereka sendiri (ENISA, 2016).

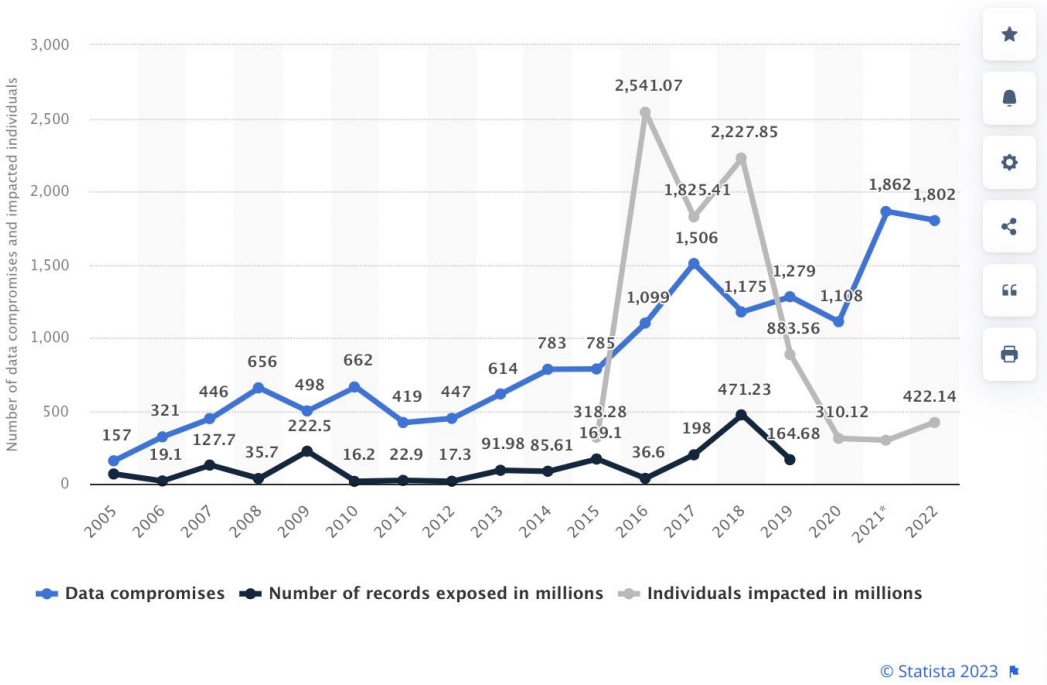
Tabel 2
Sebaran Sektor Tertarget Uni Eropa

No.	Sektor	Jumlah
1.	Administrasi Publik/Pemerintahan	24,21%
2.	Penyedia Layanan Digital	13,09%
3.	Publik	12,43%
4.	Layanan	11,78%
5.	Perbankan/Keuangan	8,64%
6.	Kesehatan	7,2%
7.	Transportasi	4,32%
8.	Energi	3,8%
9.	Militer	3,4%

10.	Media/Hiburan	3,27%
11.	Pendidikan	1,83%
12.	Pangan	0,92
13	*Space*	0,39%

Sumber: Diolah dari ENISA Threat Landscape, 2022

Pada kawasan Uni Eropa, ancaman dan serangan siber terus meningkat selama paruh kedua tahun 2021 dan 2022, tidak hanya dari segi vektor dan jumlah, tetapi juga dari segi dampaknya. Krisis Rusia-Ukraina juga menimbulkan era baru bagi perang siber dan *hacktivism* yang berdampak dalam konflik (ETL, 2022). Sementara di kawasan Amerika Serikat, dalam dua dekade terakhir jumlah *data breaches* meningkat hampir sepuluh kali lipat seiring dengan meningkatnya ketergantungan pada data digital.



Gambar 4. Jumlah *data compromises* dan individu terdampak di Amerika Serikat
Sumber: Statista, 2023, Annual number of data compromises and individuals impacted in the United States from 2005 to 2022

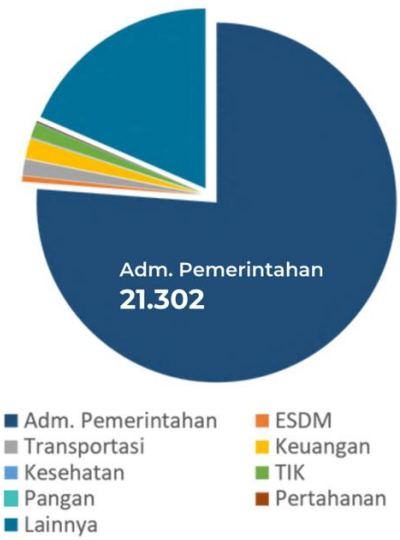
Menurut laporan Statista pada tahun 2022 jumlah *data compromises* (data terkompromi) mencapai 1802 kasus, kemudian lebih dari 422 juta individu terdampak oleh *data compromise*. Data terkompromi tersebut termasuk kebocoran, *data breaches*, dan *data exposure* yang memicu pada akses data sensitif oleh pelaku yang tidak sah (Statista, 2023). Setiap tahunnya tim CTI dari MS-ISAC secara berkala membuat rekomendasi, laporan kerentanan, sepuluh malware teratas, dan indikator-indikator kerentanan untuk menghindari ancaman dan serangan.

B. Tren Insiden Nasional

Insiden-insiden siber yang signifikan dalam dua hingga tiga tahun terakhir. Dari lanskap keamanan siber nasional tahun 2022 BSSN, mencatat bahwa terjadi 399 dugaan insiden siber pada 285 *stakeholder* yang ditangani. Jumlah insiden yang lebih banyak dari *stakeholder* disebabkan karena adanya lebih dari satu insiden yang terjadi pada *stakeholder* yang sama.

Sepanjang tahun 2022, berbagai jenis ancaman siber telah secara signifikan menargetkan ruang siber Indonesia. Insiden siber seperti kebocoran data (*data breach*) dideteksi terjadi sebanyak 311 pada 248 *stakeholder*. Sektor paling banyak dugaan kebocoran data ada Sektor Administrasi Pemerintahan, Sektor Lainnya, dan Sektor TIK. Terdapat 427 instansi di Indonesia yang terdampak *darknet exposure* dimana data atau informasi kredensial akun tersebut terekspos di *darknet* yang berpotensi untuk disalahgunakan oleh pihak yang tidak bertanggung jawab.

Sektor	Jumlah Data Exposure	Jumlah Instansi
Adm. Pemerintahan	21.302	133
ESDM	143	25
Transportasi	406	63
Keuangan	503	53
Kesehatan	17	42
TIK	375	29
Pangan	28	17
Pertahanan	14	8
Lainnya	5.168	57
Total	**27.956**	**427**



Gambar 5. Rekapitulasi *Darknet Exposure* 2022
Sumber: BSSN, 2023, Lanskap Keamanan Siber Indonesia Tahun 2022

Sementara dalam Laporan Tahunan Monitoring Keamanan Siber tahun 2021, mencatat bahwa terdapat 179 laporan dari 83 *stakeholder*. Laporan tersebut terdiri atas: *data breach, ransomware, profiling, web defacement, malicious activity, dark web enabled crime, compromised account,* dan *web phishing.* Terdapat 37 *stakeholder* yang dilakukan pendalaman, dan sebanyak 50 *threat actor* telah di-*profiling.*

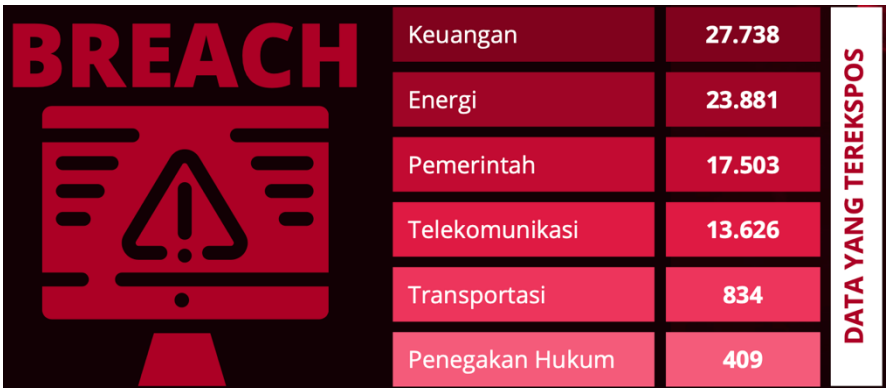
Tabel 3
Sebaran Sektor Terdampak di Indonesia Tahun 2021 dan 2022

Laporan Tahun 2022			**Laporan Tahunan 2021**	
No.	**Sektor**	**Jumlah**	**Sektor**	**Jumlah**
1.	Administrasi Pemerintahan	120	Pemerintahan	41

2.	Energi dan Sumber Daya Mineral (ESDM)	20	Pendidikan	10
3.	Teknologi Informasi dan Komunikasi (TIK)	25	Keuangan	8
4.	Pertahanan	20	*E-Commerce*	6
5.	Transportasi	13	Kesehatan	5
6.	Keuangan	14	Swasta	5
7.	Kesehatan	11	Media Sosial	4
8.	Pangan	3	Jasa Ekspedisi	3
9.	Lainnya	59	Energi	1
Total Sektor		285	**Total Sektor**	83

Sumber: BSSN, 2023

Menurut informasi dari laporan *darknet exposure* dan laporan kasus *data breach* yang telah dicatat BSSN, ditemukan data yang terekspos sebanyak 83.991. Terdapat 78 instansi yang terekspos dengan rincian sebagai berikut: 60 instansi pemerintahan, 5 instansi penegak hukum, 5 instansi energi, 4 instansi keuangan, 3 instansi transportasi, dan 1 instansi telekomunikasi. Sementara rincian data yang terekspos dapat dilihat pada gambar berikut.



Gambar 6. Rekapitulasi *Darknet Exposure* 2021
Sumber: BSSN, 2022, Laporan Tahunan Monitoring Keamanan Siber 2021

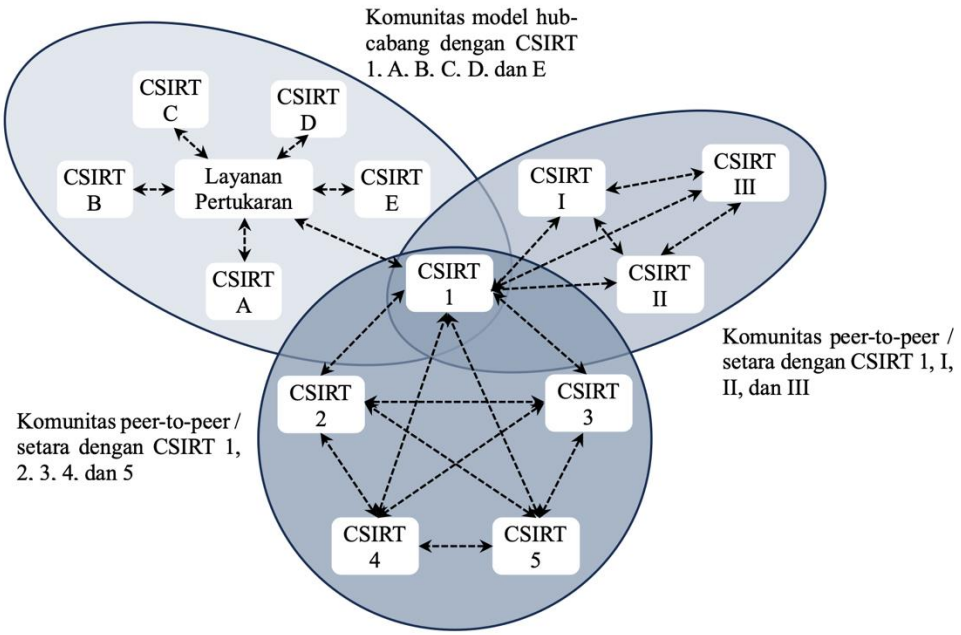
Melihat dari (BSSN, 2022) dan (BSSN, 2021) terkait laporan intelijen keamanan siber di Indonesia, jumlah sebaran *stakeholder* dugaaan insiden meningkat signifikan yakni 122,9%, jumlah *threat actor* yang di-*profiling* meningkat hampir tiga kali lipat dari 50 menjadi 138, sementara jumlah jenis insiden yang menimpa semakin kompleks dan canggih terutama varian *ransomware,* jumlah *data breach,* dan kegiatan. Rekapitulasi data terekspos pada tahun 2022 didominasi pada sektor Administrasi Pemerintahan, yakni 21.302, dan pada tahun 2021 didominasi pada sektor keuangan, yakni 27.738. Kemudian jika melihat dari (ETL, 2022) laporan intelijen keamanan siber di kawasan Eropa, ancaman dan serangan siber meningkat dalam dua tahun terakhir baik dari segi vektor,

jumlah dan dampak serangan, ditambah dengan krisis Rusia-Ukraina menimbulkan situasi baru terhadap isu geopolitik yang berdampak pada *cyber warfare* dan *hacktivism*. Di Amerika Serikat, jumlah *data breaches* meningkat hampir sepuluh kali lipat dalam dua dekade terakhir (Statista, 2023). Secara global, jumlah pencurian data meningkat dengan signifikan, identifikasi Kelompok Ancaman baru terasosiasi ke APT yang menggunakan malware secara canggih (M-Trends, 2023).

C. Usulan *Collaborative Sharing* CTI

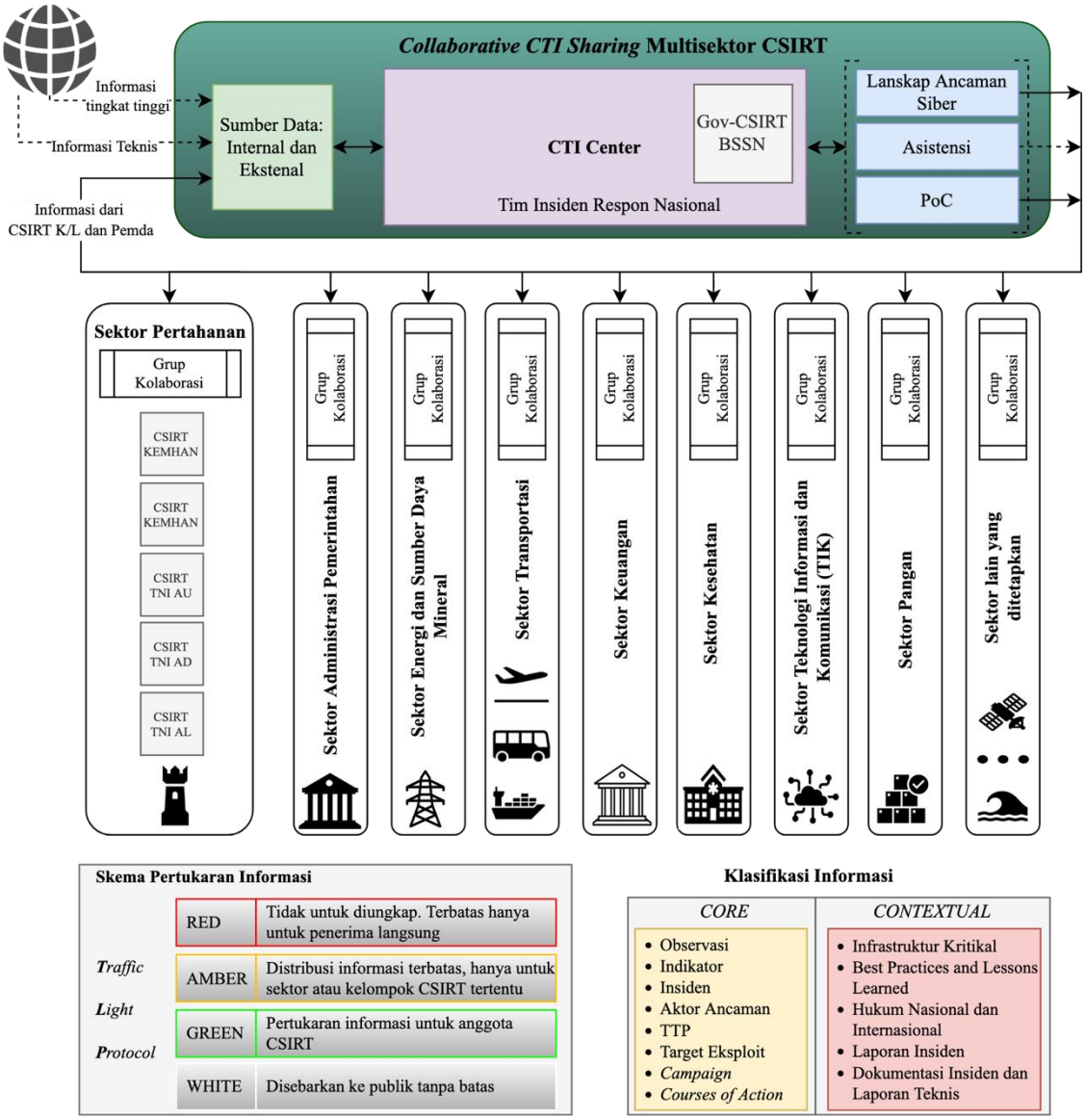
Saat ini, kebutuhan untuk operasionalisasi intelijen ancaman siber meningkat secara signifikan dalam tataran global. Dalam laporan Global Perspective on Threat Intelligence dari Mandiant, sejumlah 85% merasa perlu untuk mengidentifikasi *attacker,* dan 88% ingin mengetahui alat dan teknik yang digunakan pelaku serangan. operasionalisasi ini mempengaruhi tim keamanan dalam waktu dan kinerja, sejumlah 79% dapat lebih fokus pada waktu dan energi untuk mengidentifikasi tren-tren ancaman siber penting. Kemudian, sejumlah 89% memerlukan perubahan pada strategi keamanan siber yang berdasarkan intelijen ancaman terbaru (Mandiant, 2023). Intelijen ancaman siber sangat signifikan membantu tim keamanan dalam merespon serangan maupun tren ancaman terbaru.

Kolaborasi intelijen ancaman siber (CTI) idealnya sampai pada level teknis. Dimana setiap agen intelijen dalam hal ini para analis ancaman (*cyber security analyst*) yang bekerja di CSIRT masing-masing organisasi dapat dengan maksimal bekerja baik internal maupun dengan eksternal dengan didukung infrastruktur dan teknologi yang memadai. Kolaborasi intelijen ancaman siber dapat disesuaikan dengan kebutuhan masing-masing sektor sesuai dengan kebutuhannya. Klasifikasi ini disesuaikan dengan tugas atau layanan organisasi. Klasifikasi organisasi pemerintahan dapat diatur sesuai pembagian sektor yang diatur dalam Peraturan Presiden (PERPRES) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) yang mengatur sektor-sektor yang meliputi: Administrasi Pemerintahan, Energi dan Sumber Daya Mineral, Transportasi, Keuangan, Kesehatan, Teknologi Informasi dan Komunikasi, Pangan, Pertahanan, dan sektor lain yang ditetapkan oleh Presiden.



Gambar 7. Contoh Kolaborasi Pertukaran CTI
Diadaptasi dari: *Simultaneously participating in multiple CTI sharing communities* (Fransen & Kerkdijk, 2017. Halaman 204).

Kolaborasi pertukaran informasi intelijen ancaman harus dikelola secara hati-hati karena hal tersebut tidaklah mudah. Selain memilih platform yang tepat yang dapat mendukung penentuan penanda dan kebijakan pertukaran informasi sensitif seperti Lalu Lintas Protokol atau *Traffic Light Protocol* (TLP) dan Kebijakan Pertukaran Informasi atau *Information Exchange Policy* (IEP). Masing-masing member dalam hal ini CSIRT bisa saja berbeda dalam pemilihan platform CTI, namun alangkah lebih baik jika menggunakan lebih dari satu platform berbagi CTI ke luar dan sinkronisasi dengan internal (Fransen & Kerkdijk, 2017). Beberapa platform yang populer untuk berbagi diantaranya, Malware Information Sharing Platform (MISP), Cyber Threat Exchange, dan ThreatConnect. Dalam implementasinya, pengembangan skema pertukaran CTI kolaboratif antar CSIRT pada masing-masing sektor yang telah diatur dalam PERPRES No. 82 Tahun 2022 tentang Pelindungan IIV dapat digambarkan sebagai berikut. Administrasi Pemerintahan, Energi dan Sumber Daya Mineral, Transportasi, Keuangan, Kesehatan, Teknologi Informasi dan Komunikasi, Pangan, Pertahanan, dan sektor lain.



Gambar 8. Pertukaran kolaboratif CSIRT Multisektor CSIRT Pemerintah

Kesimpulan

Menghadapi ancaman siber saat ini, sistem peringatan dini sangat penting. Strategi reaktif harus dikombinasi dengan strategi proaktif dan preventif, yakni pemanfaatan intelijen ancaman siber (CTI). Namun bagaimanapun, pertukaran kolaboratif CTI menjadi solusi yang penting karena informasi ancaman siber dan karakteristik penyerang dapat dibagikan antar sektor dalam komunitas. Hal ini memungkinkan masing-masing CSIRT pemerintah dapat mengambil langkah-langkah proaktif dalam melindungi diri. Saat ini program CTI ada di BSSN namun distribusi informasi dan kerjasama intelijen ancaman masih terbatas.

Pengembangan *collaborative sharing* CTI harus selaras dengan peraturan yang terbaru, misalnya seperti yang diatur pada PERPRES Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) yang mengatur keamanan siber dalam

sektor-sektor yang meliputi: Administrasi Pemerintahan, Energi dan Sumber Daya Mineral, Transportasi, Keuangan, Kesehatan, Teknologi Informasi dan Komunikasi, Pangan, Pertahanan, dan sektor lain yang ditetapkan oleh Presiden.

Pertukaran kolaboratif intelijen ancaman siber multisektoral belum terimplementasi di sektor pemerintahan Indonesia. Pengembangan pertukaran kolaboratif CTI perlu dijalankan dengan memanfaatkan CSIRT yang sudah ada. Adapun saran dalam penelitian ini adalah pertukaran kolaboratif CTI dapat dijadikan sebagai ujicoba awal dalam upaya pembentukan lembaga pertukaran informasi ancaman siber yang lebih luas seperti CERT Nasional atau *Information Sharing and Analysis Center* (ISAC) Nasional di Indonesia.

BIBLIOGRAFI

Alfikri, M., & Ahmad, I. (2022). The Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, *6*(1), 1-14.

Alit Wahyudiana, A. A. P. (2023). Launching Kemenag - CSIRT, Menag: Ikuti Arahan, Kita Besarkan Pusaka. Bimashindu. https://bimashindu.kemenag.go.id/berita-pusat/launching-kemenag-csirt-menag-ikuti-arahan-kita-besarkan-pusaka-o1EeA (Tanggal akses: 17 Oktober 2023)

Ardiansyah, H., & Amalia, R. (2023). Pengenalan Cyber Security Untuk Siswa/Siswi SMP Muhammadiyah Parakan Di Era Society 5.0. *Jurnal Indimas*, *1*(1), 9-13.

Aruman, Edhy. (2023, Mei 15). Belajar Dari Krisis Bsi: Antara Keamanan Siber dan Komunikasi Krisis. Sumber: https://mix.co.id/corcomm-pr/belajar-dari-krisis-bsi-antara-keamanan-siber-dan-komunikasi-krisis/. Diakses pada 20 Juni 2021.

Badan Siber dan Sandi Negara Indonesia (BSSN). (2023). Lanskap Keamanan Siber Indonesia 2022.

Badan Siber dan Sandi Negara. (s.d.). Layanan Gov-CSIRT. Diakses pada 16 November 2023, dari https://www.bssn.go.id/gov-csirt/

Barnea, A. (2020). Strategic intelligence: a concentrated and diffused intelligence model. *Intelligence and National Security*, *35*(5), 701-716.

BBC News Indonesia. (2023, Mei 16). BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank 'tidak kuat'. Sumber: https://www.bbc.com/indonesia/articles/cn01gdr7eero. Diakses 16 Juni 2023.

Benson, M. (2022). *Towards a Research Guide for Cyber Threat Intelligence* (Doctoral dissertation, Utica University). Berlin, Heidelberg: Springer Berlin Heidelberg.

BSSN. (2023, May 30). BSSN dan BPKP Kolaborasi Launching CSIRT Sebagai Bagian Ketahanan Siber Nasional. https://www.bssn.go.id/bssn-dan-bpkp-kolaborasi-launching-csirt-sebagai-bagian-ketahanan-siber-nasional/

Burhan, F. A. (Penulis), & Setyowati, D. (Editor). (2021, 25 Juni). Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun. Katadata. https://katadata.co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun

Fransen, F., & Kerkdijk, R. (2017). Cyber threat intelligence sharing through national and sector-oriented communities. *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*, 187.

Leitner, M., Pahi, T., & Skopik, F. (2017). Situational Awareness for Strategic Decision Making on a National Level. *in Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*, 225-276.

Liu, M., Xue, Z., He, X., & Chen, J. (2019). Cyberthreat-intelligence information sharing: Enhancing collaborative security. *IEEE Consumer Electronics Magazine*, *8*(3), 17-22.

M-Trends. (2023). Mandiant Special Report. Goo**g**le Services. https://services.google.com/fh/files/misc/m_trends_2023_report.pdf

Miranda Lopez, E. (2021). A Framework to Establish aThreat Intelligence Program.

NIST. (s.d.). Computer Security Incident Response Team (CSIRT). Diakses pada 15 Oktober 2023, dari https://csrc.nist.gov/glossary/term/computer_security_incident_response_team

Pahi, T., & Skopik, F. (2017). A Systematic Study and Comparison of Attack Scenarios and Involved Threat Actors. In *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level* (pp. 19-68). CRC Press.

Putra, F. A. (2022). Pembentukan Ekosistem Local Government Information Sharing and Analysis Center (LocalGov-ISAC) dengan Toolkit ENISA ISAC in a Box pada Sektor Pemerintah Daerah Indonesia. *Info Kripto, 16*(3), 95-102.

Republika. (2023, 12 Mei). Lumpuh Empat Hari, Layanan Perbankan BSI Akhirnya Pulih. https://www.republika.id/posts/40653/lumpuh-empat-hari-layanan-perbankan-bsi-akhirnya-pulih

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 23(16), 7273.

Sakellariou, G., Fouliras, P., Mavridis, I., & Sarigiannidis, P. (2022). A reference model for cyber threat intelligence (CTI) systems. *Electronics*, *11*(9), 1401.

Schlette, D. (2021). Cyber threat intelligence. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1-3).

Schroers, J., & Clifford, D. (2017). Legal Implications of Information Sharing. In *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level* (pp. 277-312). CRC Press.

Skopik, F., Settanni, G., & Fiedler, R. (2017). The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats 1. In *Collaborative Cyber Threat Intelligence* (pp. 129-186). Auerbach Publications.