Pertukaran Informasi Keamanan Siber untuk Mendukung Kolaborasi Global

Hapsari Tilawah 23214005

Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Indonesia
13509027@std.stei.itb.ac.id

Abstrak

Ancaman siber melintasi batas negara, namun kebanyakan negara/organisasi saat ini menghadapinya secara individu tanpa kolaborasi global terutama karena kurangnya standar global untuk kerangka kerja dan format pertukaran informasi keamanan siber. Meskipun terdapat beberapa standar lokal atau industri untuk memecahkan masalah ini, standar-standar ini tidak diatur agar setiap organisasi sepenuhnya bekerja sama satu sama lain. Tulisan ini membahas ontologi informasi operasional keamanan siber untuk membangun dasar kerangka kerja pertukaran informasi keamanan siber. Tulisan ini juga membahas aktivitas standardisasi dalam pertukaran informasi keamanan siber seperti CYBEX serta mendiskusikan kegunaan dan penerapan dari ontologi dan CYBEX.

Kata kunci— operasi keamanan siber, pertukaran informasi, ontologi, CYBEX

1 Pendahuluan

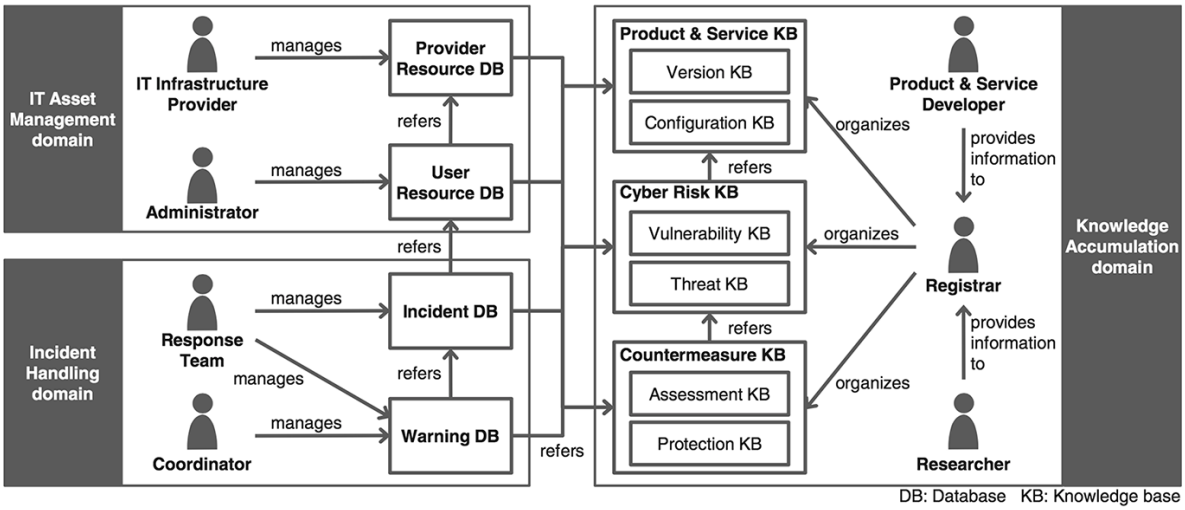
Akses Internet telah menjadi semakin meluas secara global, namun keamanan siber masih dalam proses pengembangan. Sumber ancaman siber telah melintasi batas negara dan bahkan benua, penyerang dapat menyerang komputer di negara A dengan mengendalikan komputer di negara B sementara secara fisik berada di negara C [7]. Namun, penanggulangan serangan dilaksanakan oleh masing-masing negara atau organisasi secara terpisah tanpa kolaborasi global [6]. Selain itu berdasarkan hasil survei pada [2], 54% pertukaran/*sharing* informasi antar organisasi dilaksanakan melalui surel, telepon, atau pertemuan secara fisik, oleh karenanya sangat tidak efisien.

Tabel 1: Spesifikasi industri [7]

Nama Spesifikasi	Singkatan	Organisasi
Asset Reporting Format	ARF	NIST
Common Attack Pattern Enumeration and Classification	CAPEC	ITU-T
Common Configuration Enumeration	CCE	NIST
Common Configuration Scoring System	CCSS	NIST
Common Event Expression	CEE	MITRE
Common Platform Enumeration	CPE	NIST
Common Result Format	CRF	MITRE
Common Vulnerabilities and Exposures	CVE	ITU-T
Common Vulnerability Reporting Framework	CVRF	ICASI
Common Vulnerability Scoring System	CVSS	ITU-T
Common Weakness Enumeration	CWE	ITU-T
Common Weakness Scoring System	CWSS	MITRE
Cyber Observable eXpression	CybOX	MITRE
Incident Object Description Exchange Format	IODEF	IETF
Malware Attribute Enumeration and Characterization	MAEC	ITU-T
Malware Metadata Exchange Format	MMDEF	IEEE
Open Checklist Interactive Language	OCIL	NIST
Open Vulnerability and Assessment Language	OVAL	ITU-T
Software Identification	SWID	ISO/IEC
Web Services Agreement Specification	WS-Agreement	Open Grid Forum
eXtensible Access Control Markup Language	XACML	OASIS
eXtensible Configuration Checklist Description Format	XCCDF	ISO/IEC

Salah satu penyebab dari situasi ini adalah kurangnya kerangka kerja dan format global yang umum untuk pertukaran informasi [6]. Kerangka kerja dan format seperti ini menghilangkan kesenjangan antar daerah atas informasi keamanan siber yang tersedia dalam skala global [6]. Hal ini akan memungkinkan negara-negara yang masih dalam proses mengembangkan keamanan siber dan belum mengumpulkan banyak informasi untuk lebih mudah mendapatkan informasi, juga secara signifikan mengurangi serangan siber yang memanfaatkan komputer di negara-negara tersebut untuk menargetkan komputer di negara-negara maju [6]. Format dan kerangka kerja juga mengotomatisasi operasi sehingga dapat mengurangi tenaga kerja manusia yang dibutuhkan untuk operasi juga menghindari *human error*.

Meskipun terdapat berbagai spesifikasi industri atau standar global untuk format pertukaran informasi sepeti yang ditunjukkan pada Tabel 1, standar-standar ini tidak diatur agar setiap organisasi sepenuhnya bekerja sama satu sama lain [6]. Dalam situasi saat ini tidak mungkin untuk membangun sebuah skema universal untuk semua jenis informasi keamanan siber karena skema yang diinginkan tergantung pada penggunaan informasinya [7]. Untuk mengatasi masalah ini dan untuk membangun dasar dari pertukaran informasi keamanan siber secara global, para peneliti dari Jepang dalam [6–8] mengusulkan ontologi informasi operasional keamanan siber. Ontologi adalah sebuah model konseptual dari dunia dan diharapkan akan memfasili-



Gambar 1: Ontologi dari informasi operasional keamanan siber [7]

tasi pertukaran/penggunaan kembali informasi antar perangkat lunak [7]. Ontologi tersebut didasarkan pada hasil diskusi dengan penyedia operasi keamanan siber secara aktual di Jepang, Amerika Serikat, dan Korea.

Tulisan ini menjelaskan ontologi informasi operasional keamanan siber pada Bagian 2. Bagian 3 membahas aktivitas standardisasi dari kerangka kerja pertukaran informasi keamanan siber seperti CYBEX. Bagian 4 mendiskusikan kegunaan dan penerapan dari ontologi dan CYBEX. Terakhir, Bagian 5 menyimpulkan tulisan ini.

2 Ontologi Informasi Keamanan Siber

Ontologi informasi keamanan siber mendefinisikan domain operasi, peran yang diperlukan dalam setiap domain, dan informasi yang ditangani oleh peran tersebut [6], seperti yang diilustrasikan dalam Gambar 1. Formalisasi dari ontologi ini dapat dilihat pada [7], formalisasi bertujuan untuk mengurangi ambiguitas. Bagian ini membahas domain operasi, peran, dan informasi keamanan siber dalam ontologi sebagaimana yang dibahas pada [7].

2.1 Domain Operasi

Istilah 'operasi keamanan siber' mencakup berbagai operasi keamanan dalam masyarakat siber, namun fokus dalam tulisan ini adalah pada operasi keamanan siber yang menjaga keamanan informasi dalam masyarakat siber. Untuk merepresentasikan domain dari operasi tersebut, ontologi mendefinisikan tiga domain operasi: IT Asset Management, Incident Handling, dan Knowledge Accumulation.

IT Asset Management menjalankan operasi keamanan siber dalam organisasi pengguna

seperti menginstal, mengkonfigurasi dan mengelola aset TI, serta meliputi pencegahan insiden dan operasi pengendalian kerusakan. Aset TI tidak hanya mencakup aset TI pengguna sendiri tetapi juga konektivitas jaringan, *cloud service*, dan layanan identitas yang diberikan oleh entitas eksternal untuk pengguna.

Incident Handling mendeteksi dan merespon insiden yang terjadi dalam masyarakat siber dengan memantau kejadian komputer, insiden yang terdiri dari beberapa kejadian, dan perilaku serangan yang menyebabkan insiden. Kejadian komputer dipantau kemudian dihasilkan laporan insiden ketika sebuah anomali terdeteksi. Berdasarkan laporan, insiden diselidiki secara detil sehingga dapat diketahui pola serangan dan penanggulangannya. Berdasarkan analisis insiden, peringatan dan saran dapat diberikan, misalnya peringatan dini terhadap ancaman potensial kepada organisasi pengguna.

Knowledge Accumulation mengumpulkan dan menghasilkan informasi keamanan siber dan mengekstrak pengetahuan yang dapat digunakan kembali untuk organisasi lainnya. Untuk memfasilitasi *reusability*, Knowledge Accumulation menyediakan penamaan dan taksonomi umum, yang dengan hal tersebut pengetahuan diatur dan diakumulasikan. Domain ini berfungsi sebagai dasar kolaborasi global di luar batas organisasi.

2.2 Peran

Berdasarkan domain operasi yang didefinisikan dalam Bagian 2.1, bagian ini mengidentifikasi peran yang diperlukan untuk menjalankan operasi keamanan siber di setiap domain. Domain IT Asset Management memiliki Administrator dan IT Infrastructure Provider, domain Incident Handling memiliki Response Team dan Coordinator, serta domain Knowledge Accumulation memiliki Researcher, Product & Service Developer, dan Registrar. Perhatikan bahwa peran didefinisikan dari sudut pandang fungsi. Oleh karena itu, satu entitas dapat melakukan beberapa peran tergantung pada konteksnya.

Administrator mengelola sistem organisasi dan mempertahankan fungsionalitasnya. Untuk tujuan ini, peran ini memonitor penggunaan sistem, mendiagnosis sistem dengan menjalankan pemeriksaan integritas, pemindaian kerentanan dan menjalankan tes penetrasi, kemudian menilai tingkat keamanan sistem. Contoh tipikal dari peran ini adalah seorang administrator sistem dalam setiap organisasi. Managed Security Service Provider (MSSP) juga berfungsi sebagai Administrator jika sebuah organisasi melakukan *outsourcing* beberapa operasi di atas.

IT Infrastructure Provider menyediakan infrastruktur TI yang tepat (termasuk sumber daya dan layanan) untuk sebuah organisasi. Infrastruktur meliputi konektivitas jaringan dan *cloud service* seperti *software as a service* (SaaS), *platform as a service*, dan *infrastructure as a*

service. Peran ini mempertahankan kualitas dan keamanan dari infrastruktur sehingga organisasi pengguna dapat menikmati yang terbaik dari infrastrukturnya. Misalnya, IT Infrastructure Provider menerapkan kontrol akses, memonitor log akses, dan mengontrol arus lalu lintas pada jaringan. Contoh tipikal dari peran ini adalah penyedia layanan Internet, penyedia layanan aplikasi, dan penyedia *cloud service*.

Response Team memonitor dan menganalisis kejadian dalam sebuah organisasi. Response Team mendeteksi insiden, misalnya akses yang tidak sah, serangan *distributed denial of service* (DDoS), dan *phishing*, kemudian mengakumulasikan informasi insiden. Response Team juga menjalankan triase (atau kadang-kadang remediasi) pada insiden tersebut dengan berkolaborasi dengan Administrator atau IT Infrastructure Provider. Sebagai contoh, Response Team dapat meminta administrator dari organisasi pengguna untuk mengisolasi komputernya dari jaringan, atau mungkin meminta penyedia jaringan untuk mendaftarkan alamat situs *phishing* di-*blacklist* atau memblokir lalu lintas yang berbahaya. Contoh tipikal dari peran ini adalah tim respon insiden dalam sebuah MSSP. Dalam banyak organisasi pengguna, administrator sistem sering bekerja tidak hanya sebagai Administrator tetapi juga sebagai Response Team.

Coordinator berkoordinasi dengan peran lain dan membahas potensi ancaman berdasarkan insiden yang dikenal dan informasi kejahatan. Coordinator memberikan peringatan kepada organisasi lain dan kadang-kadang memimpin mitigasi kolaboratif untuk menangani serangan yang dahsyat dan berskala besar seperti serangan DDoS. Kolaborasi antara Response Team, Administrator, dan IT Infrastructure Provider sering kali membutuhkan koordinasi yang disediakan oleh Coordinator, jika peran-peran tersebut dimiliki oleh organisasi yang berbeda. Contoh tipikal dari peran ini adalah CERT Coordination Center (CERT/CC), baik itu komersial atau non-komersial.

Researcher meneliti masalah keamanan siber termasuk kerentanan dan serangan, mengekstrak pengetahuan dari penelitian dan mengakumulasikan pengetahuan. Researcher mempublikasikan banyak informasi yang *reusable* melalui Registrar sehingga organisasi secara individu dapat mengimplementasikan penanggulangan yang diperlukan. Contoh tipikal dari peran ini adalah X-force dalam International Business Machines Corp. (IBM), Risk Research Institute of Cyber Space pada Little eArth Corporation Co., Ltd. (LAC), dan McAfee Lab dalam McAfee, Inc.

Product & Service Developer mengembangkan produk dan layanan serta mengakumulasikan informasi tentangnya, seperti versi, konfigurasi, kerentanan dan *patch*-nya. Peran ini mempublikasikan banyak informasi yang *reusable* melalui Registrar sehingga, sama seperti Researcher, organisasi secara individu dapat mengimplementasikan penanggulangan yang di-

perlukan. Contoh tipikal dari peran ini adalah sebuah vendor perangkat lunak dan pemrogram perangkat lunak swasta secara individu.

Registrar mengklasifikasikan, mengatur, dan mengakumulasikan pengetahuan keamanan siber yang disediakan oleh Researcher dan Product & Service Developer sehingga pengetahuan dapat digunakan kembali oleh organisasi lain. Contoh tipikal dari peran ini adalah NIST dan IT Promotion Agency, Jepang. Dalam beberapa kasus, entitas yang berfungsi sebagai Researcher dan Product & Service Developer juga dapat berfungsi sebagai Registrar dan mempublikasikan informasi.

2.3 Informasi Keamanan Siber

Berdasarkan domain operasi dan peran, bagian ini mengidentifikasikan informasi keamanan siber yang diperlukan untuk operasi. Dengan mempertimbangkan informasi yang mana masing-masing peran terlibat, didefinisikan empat basis data (User Resource, Provider Resource, Incident, dan Warning) dan tiga basis pengetahuan (Product & Service, Cyber Risk, dan Countermeasure). Perhatikan bahwa basis data dan basis pengetahuan sama-sama mengumpulkan informasi, bedanya adalah sebagian besar informasi dalam basis data tidak cukup disempurnakan untuk dibagikan dan digunakan kembali oleh organisasi lain, sedangkan sebagian besar informasi dalam basis pengetahuan sudah cukup disempurnakan untuk dibagikan dan digunakan kembali oleh organisasi lain.

2.3.1 User Resource Database

Basis data ini menyimpan informasi tentang aset dalam sebuah organisasi. Informasi tersebut biasanya terdiri dari daftar perangkat lunak/perangkat keras, konfigurasinya, status penggunaan sumber daya, hasil penilaian tingkat keamanan, topologi Intranet, data *provenance*, kebijakan keamanan informasi termasuk kebijakan kontrol akses, serta standar dan pedoman keamanan informasi yang digunakan organisasi tersebut. Basis data ini juga berisi informasi sumber daya eksternal yang organisasi pengguna gunakan seperti daftar layanan *online* langganan (misalnya *data center* dan SaaS) dan catatan penggunaannya. Basis data ini dikelola oleh Administrator. ARF dapat digunakan untuk menggambarkan aset TI dalam sebuah organisasi, XACML dapat digunakan untuk menggambarkan kebijakan kontrol akses, sedangkan CVSS/CWSS dapat digunakan untuk menilai skor tingkat keamanan aset TI. Skor tingkat keamanan aset TI berguna untuk Administrator dalam memprioritaskan urgensi operasi keamanan aset TI.

2.3.2 Provider Resource Database

Basis data ini menyimpan informasi yang diperlukan oleh organisasi pengguna untuk menjalankan operasi operasi keamanan siber. Basis data ini dimiliki dan dikelola oleh IT Infrastructure Provider. Basis data secara pokok berisi informasi tentang jaringan, aset server dan kebijakan. Informasi jaringan terkait dengan jaringan yang mana masing-masing organisasi pengguna terhubungkan, seperti topologi, informasi *routing*, kebijakan kontrol akses, status lalu lintas dan paket log. Informasi aset server termasuk log akses, catatan penggunaan layanan, laporan pendeteksian anomali, dan informasi beban kerja. Informasi kebijakan meliputi persyaratan dan ketentuan, spesifikasi layanan, perjanjian tingkat layanan, kebijakan keamanan informasi, serta standar dan pedoman keamanan informasi yang digunakan IT Infrastructure Provider. WS-Agreement dapat digunakan untuk menggambarkan perjanjian layanan. Perhatikan bahwa informasi spesifik organisasi pengguna seperti konfigurasi lokal masing-masing *cloud service* disimpan dalam User Resource Database. Untuk menjalankan operasi keamanan siber yang efektif dan efisien, basis data ini perlu dikaitkan dengan User Resource Database. Oleh karena itu, batasan antara aset internal dan eksternal TI menjadi semakin tidak jelas, terutama dalam *cloud computing*.

2.3.3 Incident Database

Basis data ini berisi informasi tentang insiden yang dihasilkan terutama dari analisis informasi dalam User Resource Database. Response Team mengelola informasi dalam basis data ini. Basis data ini mencakup tiga catatan: Event Record, Incident Record, dan Attack Record.

Event Record berisi informasi tentang kejadian komputer termasuk dalam paket, berkas, dan transaksinya. Biasanya komputer secara otomatis memberikan sebagian besar catatan sebagai log komputer, seperti waktu dan tanggal *log-in* serta informasi terminal yang tersedia ketika pengguna *root* melakukan *log-in* ke sistem. Log adalah contoh dari catatan ini. CEE dan CybOX dapat digunakan untuk menggambarkan catatan ini.

Incident Record berisi informasi tentang insiden keamanan dan memberikan informasi seperti *current state* sistem pengguna dan risiko lebih lanjut. Catatan ini berasal dari analisis beberapa Event Records dan dugaannya, yang dibuat secara otomatis atau manual. Misalnya, ketika akses berlebih untuk satu komputer terdeteksi, *state* dari komputer (akses berlebih untuk satu komputer) dan ekspektasi konsekuensinya (*denial of service*) harus dicatat dalam Incident Record. Sejauh mana kerusakan yang disebabkan oleh insiden serta kebutuhan untuk penanggulangan dapat diperkirakan dari catatan ini yang disesuaikan dengan kebijakan, standar, dan pedoman keamanan informasi. Perhatikan bahwa Incident Record dapat merekam insiden yang

salah (*false positive*); yaitu kandidat insiden yang dinilai sebagai non-insiden setelah dilakukan penyelidikan. IODEF dapat digunakan untuk menggambarkan catatan ini.

Attack Record berisi informasi tentang serangan yang berasal dari analisis Incident Records. Catatan ini menggambarkan urutan serangan; seperti bagaimana serangan itu dimulai, aset TI mana yang ditargetkan, dan bagaimana tersebarnya kerusakan yang diakbatkan serangan itu. Perhatikan bahwa catatan ini perlu dikaitkan dengan Incident Record.

2.3.4 Warning Database

Basis data ini berisi informasi tentang peringatan keamanan siber. Informasi ini dirancang baik untuk masyarakat umum atau organisasi tertentu. Informasi untuk masyarakat umum biasanya terdiri dari informasi statistik dan peringatan, sementara informasi untuk organisasi tertentu terdiri dari kebijakan dan pedoman keamanan serta saran keamanan yang disesuaikan untuk organisasi. Informasi ini dihasilkan terutama dari informasi dalam Incident Database dan Cyber Risk Knowledge Base. Coordinator dan Response Team mengelola informasi dalam basis data ini. Berdasarkan pada peringatan, organisasi pengguna dapat mengimplementasikan penanggulangan terhadap risiko keamanan siber yang diperingatkan.

2.3.5 Product & Service Knowledge Base

Basis pengetahuan ini mengumpulkan informasi tentang produk dan layanan. Informasi ini disediakan oleh Researcher dan Product & Service Developer, kemudian diatur dan diklasifikasikan oleh Registrar. Basis pengetahuan ini mencakup Version Knowledge Base dan Configuration Knowledge Base.

Version Knowledge Base mengumpulkan informasi versi dari produk dan layanan, yang meliputi penamaan dan penghitungan versinya. *Patch* keamanan dari produk perangkat lunak juga disertakan di sini. Identifier CPE dan label SWID dapat digunakan untuk menghitung aset perangkat lunak dan platform.

Configuration Knowledge Base mengumpulkan informasi konfigurasi dari produk dan layanan, termasuk penamaan, taksonomi dan penghitungan konfigurasi yang diketahui dari produk dan layanan. Terkait dengan konfigurasi layanan, informasi juga berisi pedoman untuk penggunaan layanan. CCE dapat digunakan untuk menghitung konfigurasi umum dari produk.

2.3.6 Cyber Risk Knowledge Base

Basis pengetahuan ini mengumpulkan informasi risiko keamanan siber. Informasi ini disediakan oleh Researcher dan Product & Service Developer, kemudian diatur dan diklasifikasikan oleh Re-

gistrar, seperti pada basis pengetahuan lainnya. Basis pengetahuan ini mencakup Vulnerability Knowledge Base dan Threat Knowledge Base.

Vulnerability Knowledge Base mengumpulkan informasi kerentanan yang diketahui umum, meliputi penamaan, taksonomi, dan penghitungan dari perangkat lunak yang diketahui dan sistem kerentanan. Informasi kerentanan meliputi kerentanan yang disebabkan oleh pemrograman dan konfigurasi. Basis pengetahuan ini juga mencakup informasi tentang kerentanan manusia, yaitu kerentanan pada pengguna IT manusia. CVE dan CWE dapat digunakan untuk menggambarkan isi dari basis pengetahuan ini.

Threat Knowledge Base mengumpulkan informasi ancaman keamanan siber yang diketahui umum. Basis pengetahuan ini memiliki pengetahuan tentang serangan dan penyalahgunaan. Pengetahuan serangan meliputi pola serangan, kakas serangan (misalnya *malware*), dan tren serangan (misalnya informasi statistik tentang serangan dari segi geografi, jenis organisasi target, dan kerentanan yang dieksploitasi). CAPEC dan MAEC dapat digunakan untuk menggambarkan pengetahuan serangan. Pengetahuan penyalahgunaan mencakup informasi tentang penyalahgunaan yang dikaitkan dengan penggunaan yang tidak sesuai dari pengguna, apakah berbahaya atau tidak. Penyalahgunaan yang tidak berbahaya termasuk salah ketik, kesalahpahaman, dan terkena perangkap *phishing*, sedangkan penyalahgunaan yang berbahaya termasuk pelanggaran kepatuhan seperti penggunaan layanan yang tidak sah dan akses ke materi yang tidak seharusnya.

2.3.7 Countermeasure Knowledge Base

Basis pengetahuan ini mengumpulkan informasi tentang langkah penanggulangan risiko keamanan siber. Informasi ini disediakan oleh Researcher dan Product & Service Developer, kemudian diatur dan diklasifikasikan oleh Registrar, seperti pada basis pengetahuan lainnya. Basis pengetahuan ini mencakup Assessment Knowledge Base dan Protection Knowledge Base.

Assessment Knowledge Base mengumpulkan aturan dan kriteria yang diketahui umum untuk menilai tingkat keamanan aset TI, ceklis konfigurasi dan heuristik termasuk *best practices*. CCSS, CVSS dan CWSS menyediakan rumus untuk menilai tingkat keamanan, dan hasil penilaian yang mungkin dapat digunakan kembali oleh organisasi lain (misalnya skor tingkat keparahan kerentanan) dikumpulkan dalam basis pengetahuan ini. XCCDF dan OVAL dapat digunakan untuk menggambarkan aturan dan menyediakan ceklis, dan skripnya juga dikumpulkan dalam basis pengetahuan ini.

Protection Knowledge Base mengumpulkan informasi yang diketahui umum tentang pendeteksian dan pencegahan ancaman keamanan. Basis pengetahuan ini termasuk *blacklist* URL

Tabel 2: Spesifikasi keluarga CYBEX [5]

Blok fungsional	Spesifikasi keluarga CYBEX	
	Spesifikasi yang diimpor	Spesifikasi baru
Information Description Block	Semua spesifikasi dalam Tabel 1	X.pfoc
Information Discovery Block		X.cybex.1, X.cybex-disc
Information Query Block		X.chirp
Information Assurance Block	EVCERT, TS102042 V2.0	X.eaa
Information Transport Block		X.cybex-tp, X.cybex-beep

dan daftar *open resolvers* dan server surel yang memungkinkan relai surel pihak ketiga. Basis pengetahuan ini juga termasuk tanda tangan dari *intrusion detection system* (IDS), *intrusion prevention system* (IPS), dan aturan deteksi/proteksi yang digunakan oleh tanda tangan. Basis pengetahuan ini juga mengumpulkan heuristik termasuk *best practices*.

3 Standar Pertukaran Informasi Keamanan Siber

Ontologi telah membangun sebuah platform untuk membahas siapa yang harus memiliki informasi dan jenis informasi apa yang perlu dipertukarkan. Namun, dibangunnya platform ini tidak berarti dapat memfasilitasi pertukaran informasi, oleh karenanya perlu dibangun kerangka kerja untuk mewujudkan pertukaran informasi berdasarkan pada platform ini [6]. Sebagai salah satu inisiatif untuk mencapai hal ini, ITU-T membangun standar *cybersecurity information exchange framework* (CYBEX). CYBEX yang didefinisikan dalam [1] menyediakan kerangka kerja untuk membuat struktur informasi keamanan siber dan melakukan pertukaran informasi melalui jaringan siber.

3.1 Spesifikasi CYBEX

CYBEX terdiri dari lima blok fungsional utama: Information Description, Information Discovery, Information Query, Information Assurance, dan Information Transport [5]. Setiap blok fungsional terdiri dari berbagai macam spesifikasi seperti ditunjukkan pada Tabel 2. Seperti yang dapat dilihat, salah satu karakteristik penting dari CYBEX adalah bahwa standar *de jure* ini didasarkan pada standar-standar *de facto* terkini sehingga pengguna dapat menggunakan CYBEX dengan produk-produk yang tersedia [5]. Bagian ini menjelaskan masing-masing blok fungsional sebagaimana yang dijelaskan pada [5].

Tabel 3: Spesifikasi informasi keamanan siber dalam CYBEX [5, 7]

Kategori	Format
User Resource DB	ARF, XACML
Provider Resource DB	WS-Agreement
Incident DB	CEE, CybOX
Warning DB	IODEF, X.pfoc
Cyber Risk KB	
Vulnerability KB	CVE, CVRF, CWE
Threat KB	CAPEC, MAEC, MMDEF
Countermeasure KB	
Assessment KB	CCSS, CVSS, CWSS
Protection KB	OCIL, OVAL, XCCDF
Product & Service KB	
Version KB	CPE, SWID
Configuration KB	CCE

DB: Database; KB: Knowledge Base.

3.1.1 Information Description Block

Blok fungsional ini membuat struktur informasi keamanan siber untuk tujuan pertukaran dan menyediakan format dan bahasa untuk menggambarkannya. Dari sudut pandang ontologi informasi operasional keamanan siber, spesifikasi ini diklasifikasikan seperti yang ditunjukkan pada Tabel 3.

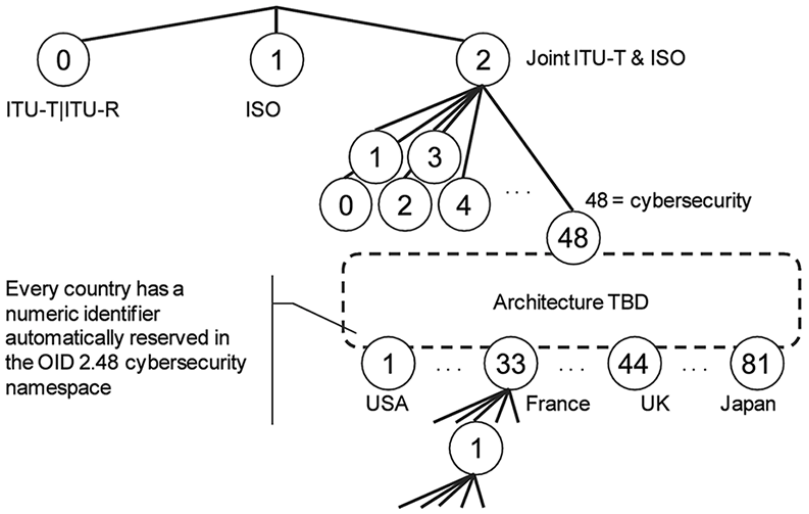
X.pfoc (Phishing, Fraud, and Other Crimeware Exchange Format) merupakan ekstensi dari IODEF untuk mendukung pelaporan *phishing*, penipuan, dan jenis-jenis kejahatan elektronik. Ekstensi ini juga mendukung pertukaran informasi tentang insiden *spam* yang tersebar luas.

3.1.2 Information Discovery Block

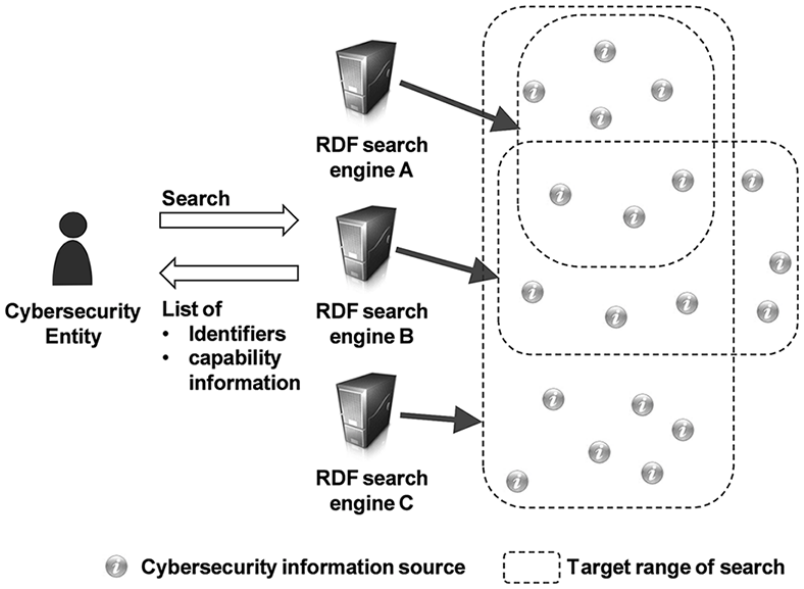
Blok fungsional ini mengidentifikasi dan menemukan informasi dan entitas keamanan siber. X.cybex-disc menyediakan metode dan mekanisme tersebut, dan memberikan dua paradigma untuk penemuan layanan dan informasi: penemuan tersentralisasi dan penemuan terdesentralisasi.

Contoh penemuan tersentralisasi adalah pohon Object Identifier (OID) dari ITU. Gambar 2 menggambarkan konsep identifikasi informasi keamanan siber dalam penemuan berbasis OID. Informasi keamanan siber diindeks secara hierarkis dalam sebuah pohon, dengan demikian informasi apapun dapat dilacak dengan menelusuri pohon.

Contoh umum dari penemuan terdesentralisasi adalah Resource Description Framework (RDF) dari W3C. RDF adalah bahasa sintaksis dan semantik untuk merepresentasikan informasi yang menjelaskan sumber daya yang tersedia. Gambar 3 menggambarkan konsep identifikasi



Gambar 2: Penemuan berbasis OID [5]



Gambar 3: Penemuan berbasis RDF [5]

informasi keamanan siber dalam penemuan berbasis RDF. Seorang pengguna yang ingin mengakses informasi menggunakan mesin pencari RDF yang memiliki daftar indeks untuk berbagai macam informasi keamanan siber dalam jaringan.

3.1.3 Information Query Block

Blok fungsional ini meminta dan merespon informasi keamanan siber. CYBEX memperkenalkan X.chirp yang menyediakan akses yang aman termasuk manajemen dan pemeliharaan informasi keamanan siber melalui seperangkat antarmuka umum. X.chirp adalah sebuah bahasa kueri yang merupakan ekstensi dari SQL.

3.1.4 Information Assurance Block

Blok fungsional ini memastikan validitas dari informasi. CYBEX memperkenalkan tiga standar: EVCERT, X.eaa dan ETSI TS102042 V2.0. EVCERT adalah draf rekomendasi untuk tanda tangan digital. X.eaa adalah draf rekomendasi untuk jaminan identitas. ETSI TS102042 V.2.0 adalah draf rekomendasi untuk kebutuhan polis untuk *certification authority* (CA).

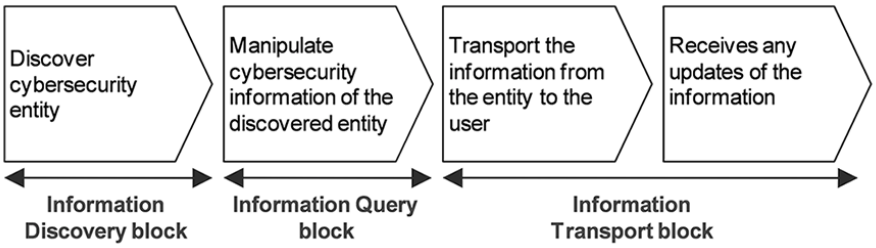
3.1.5 Information Transport Block

Blok fungsional ini melakukan pertukaran informasi keamanan siber melalui jaringan. Gambaran fungsi dijelaskan dalam X.cybex-tp. X.cybex-tp menjelaskan gambaran protokol transpor untuk pertukaran informasi keamanan informasi. Berdasarkan pada gambaran umum, fitur protokol spesifik dijelaskan dalam draf rekomendasi X.cybex-beep, yang menggambarkan protokol transpor berdasarkan BEEP.

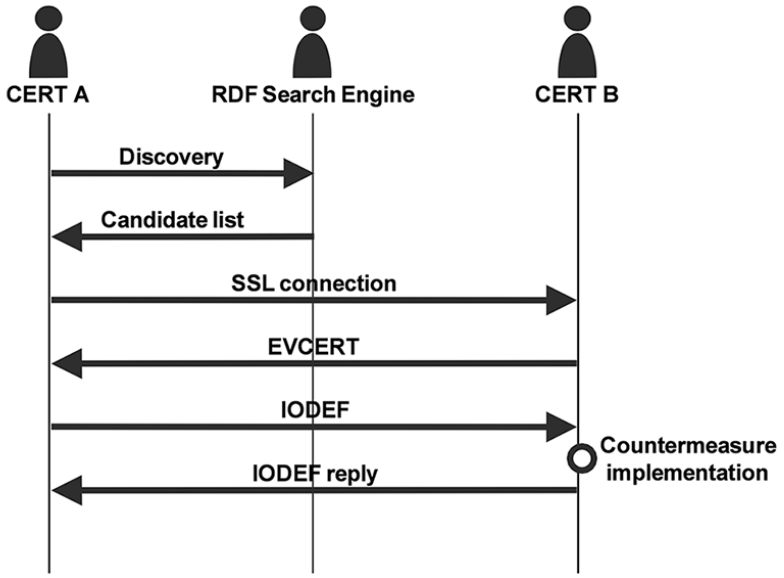
3.2 Contoh Kasus Penggunaan CYBEX

CYBEX menyediakan kerangka kerja untuk pertukaran informasi keamanan siber antar entitas keamanan siber. Bagaimana untuk mendapatkan/menggunakan informasi keamanan siber adalah di luar lingkup CYBEX [5]. Dengan demikian, penggunaan dari standar ini diserahkan sepenuhnya kepada pengguna. Bagian ini menjelaskan dua kasus penggunaan dari CYBEX seperti yang dijelaskan pada [5] untuk mendemonstrasikan penggunaan dari CYBEX.

Seorang pengguna mungkin ingin mengetahui kerentanan pada komputer tertentu dan ingin tetap *up-to-date* tentang informasi terkait komputer tersebut. Dalam hal ini, CYBEX adalah salah satu pilihan yang paling memungkinkan untuk pengguna, yang dapat menggunakan CYBEX seperti yang ditunjukkan pada Gambar 4. Pertama, pengguna mengidentifikasi masalah keamanan siber pada komputer tertentu, dan mereka ingin mengetahui lebih lanjut tentang isu dari repositori yang sesuai yang tahu tentang isu keamanan siber ini dengan menggunakan salah penemuan berbasis OID atau penemuan berbasis RDF (Information Discovery Block). Pengguna mengirimkan permintaan ke repositori untuk mendapatkan dan mengambil informasi yang diinginkan tentang isu keamanan informasi yang disimpan dalam repositori menggunakan X.chirp (Information Query Block). Informasi tersebut kemudian dapat ditransfer ke pengguna menggunakan BEEP dengan profil CYBEX (Information Transport Block) atau mekanisme transfer lainnya. Pengguna sekarang memiliki informasi yang diinginkan tentang isu keamanan informasi pada komputer tersebut menggunakan berbagai komponen CYBEX.



Gambar 4: Akuisisi informasi keamanan siber [5] untuk contoh kasus pertama



Gambar 5: Notifikasi informasi IODEF [5] untuk contoh kasus kedua

Kasus penggunaan lain adalah ketika CERT A menemukan sebuah insiden di CERT B, dan CERT A ingin menyampaikan informasi insiden tersebut ke CERT B. Dalam kasus ini, CERT A mencari CERT B menggunakan penemuan berbasis RDF (Information Discovery Block) dan menerima daftar kandidat CERT B dengan deskripsi kemampuannya. Berdasarkan informasi kemampuannya, CERT A memilih entitas yang tampaknya paling mungkin sebagai CERT B, kemudian menjalin koneksi dengan entitas melalui SSL. CERT A kemudian menerima EVCERT dari entitas sehingga CERT A dapat memastikan bahwa entitas tersebut adalah benar CERT B (Information Assurance Block). CERT A mengirimkan informasi insiden dengan format IODEF ke CERT B, kemudian CERT B membalasnya dengan pesan IODEF lain untuk melaporkan penyelesaian implementasi penanggulangan (Information Description Block). Prosedur ini digambarkan pada Gambar 5.

Gambar 6: Komunikasi tim respon insiden dengan pihak luar [3]

4 Evaluasi dan Diskusi

Pada April 2014, Ponemon Institute mengadakan survei kepada 701 praktisi TI dan keamanan TI yang familiar dan terlibat dalam aktivitas atau proses intelijen ancaman siber dalam perusahaannya [2]. Secara keseluruhan, partisipan setuju bahwa pertukaran informasi keamanan siber adalah penting. Menariknya, hasil survei mengatakan sebanyak 71% motivasi untuk melakukan pertukaran informasi keamanan siber adalah untuk meningkatkan profil keamanan siber dari organisasinya masing-masing, bukannya untuk membuat informasi ancaman lebih dapat ditindaklanjuti (24%) atau untuk meningkatkan ketepatan waktu dari data ancaman (21%). Walaupun begitu, setidaknya sudah ada itikad untuk menerapkan pertukaran informasi keamanan siber, khususnya dengan kerangka kerja CYBEX.

Informasi keamanan siber butuh untuk dibagikan ke berbagai pihak untuk meminimalisasi insiden keamanan. Sebagaimana yang direkomendasikan oleh NIST dalam [3], tim respon insiden harus mendiskusikan informasi ke berbagai pihak seperti yang ditunjukkan pada Gambar 6. Lebih jauh lagi, NIST juga merekomendasikan penggunaan basis pengetahuan agar analisis insiden lebih mudah dan lebih efektif. Dengan demikian, ontologi yang dibahas dalam tulisan ini pada dasarnya selaras dengan penanganan insiden yang direkomendasikan oleh NIST.

Ontologi memfasilitasi penstrukturan informasi keamanan siber yang membuat operasi manajemen informasi dalam organisasi menjadi lebih sederhana sehingga operasi lebih efektif dan efisien. Manajemen informasi adalah dasar dari keamanan siber dan pertahanan siber [7]. Administrator dalam organisasi dapat menyatukan pengelolaan berbagai macam informasi keamanan

dengan menggunakan ontologi dan basis pengetahuan. Dalam hal infrastruktur kritis, informasi pada sistem kontrol industri juga diperlukan untuk melindungi infrastruktur dan informasi tersebut seringkali disimpan secara terpisah dari informasi keamanan siber. Ontologi menawarkan solusi kontrol administrasi tersentralisasi atas tipe informasi semacam ini (informasi infrastruktur kritis) yaitu dengan membangun basis pengetahuan, meskipun langkah-langkah keamanan yang tepat termasuk kontrol akses perlu diterapkan untuk basis pengetahuan [7].

Terdapat berbagai macam isu yang harus ditangani untuk menerapkan pertukaran informasi keamanan siber ini, salah satunya adalah isu privasi dari data keamanan siber. Dari survei [2], sebanyak 50% mengatakan bahwa salah satu rintangan untuk mencapai kolaborasi yang lebih efektif adalah kekhawatiran akan kepercayaan. Isu hukum terkait pertukaran informasi keamanan siber juga harus ditangani. Bahkan di negara maju seperti Amerika Serikat, aspek hukum dari pertukaran informasi keamanan siber juga masih dalam perdebatan [4]. Seorang jaksa dari Amerika Serikat dalam [4] membahas bagaimana tantangan dan solusi hukum terkait pertukaran informasi keamanan siber baik antar perusahaan swasta, antar pemerintahan, maupun antara perusahaan swasta dan pemerintahan.

5 Kesimpulan

Ontologi mendefinisikan tipe informasi keamanan siber, peran, dan operasi domain, serta mengklarifikasi siapa menggunakan tipe informasi apa untuk tujuan apa. CYBEX menyediakan sebuah kerangka kerja untuk memfasilitasi pertukaran informasi keamanan siber antar entitas keamanan siber dan meminimalisasi kesenjangan ketersediaan informasi keamanan siber antar entitas. Untuk memajukan keamanan siber, efektivitas dari pertukaran informasi keamanan siber (khususnya dengan kerangka kerja CYBEX) perlu diakui secara luas dan global. Isu non-teknis seperti motivasi, isu privasi, dan isu hukum terkait dengan pertukaran informasi keamanan siber juga harus ditangani.

Referensi

[1] *ITU-T X.1500 Overview of cybersecurity information exchange.* International Telecommunications Union, Geneva, Switzerland, 2011.

[2] *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way.* Private & Confidential Report, Ponemon Institute, April 2014. `http://content.internetidentity.com/acton/attachment/8504/f-001b/1/-/-/-/-/Ponemon%20Study.pdf`.

[3] Cichonski, Paul *dkk*: *Special Publication 800-61 Revision 2 Computer security incident handling guide*. National Institute of Standards and Technology, Maryland, USA, 2012.

[4] Nolan, Andrew: *Cybersecurity and Information Sharing: Legal Challenges and Solutions*. Congressional Research Service, Maret 2015.

[5] Rutkowski, Anthony *dkk*: *CYBEX: the cybersecurity information exchange framework (x. 1500)*. ACM SIGCOMM Computer Communication Review, 40(5):59–64, 2010.

[6] Takahashi, Takeshi dan Youki Kadobayashi: *Cybersecurity Information Exchange Techniques: Cybersecurity Information Ontology and CYBEX*. Journal of the National Institute of Information and Communications Technology, 58(3/4), 2011.

[7] Takahashi, Takeshi dan Youki Kadobayashi: *Reference Ontology for Cybersecurity Operational Information*. The Computer Journal, 2014.

[8] Takahashi, Takeshi, Youki Kadobayashi, dan Hiroyuki Fujiwara: *Ontological approach toward cybersecurity in cloud computing*. Dalam *Proceedings of the 3rd international conference on Security of information and networks*, halaman 100–109. ACM, 2010.