Perancangan Proses Bisnis Diseminasi Informasi Ancaman Siber Berbasis STIX dan TAXII pada Subdirektorat Deteksi Potensi Ancaman Badan Siber dan Sandi Negara

Nusranto Pratama Tirsa[1)], Obrina Candra Briliyant[2)]

(1) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, nusranto.pratama@bssn.go.id

(2) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, obrina@polteksn.ac.id

Abstrak

Cyber Threat Intelligence (CTI) adalah sistem pengelolaan pengetahuan berbasis bukti yang dapat ditindaklanjuti. CTI dibagi menjadi 3 (tiga) bagian besar, yaitu pengumpulan informasi, analisis, serta pemanfaatan dan diseminasi. Untuk melakukan diseminasi dalam CTI, telah dikembangkan Structured Threat Information Expression (STIX) dan Trusted Automated Exchange of Intelligence Information (TAXII) sebagai standar dari platform diseminasi CTI. CTI yang efektif adalah CTI yang dapat terintegrasi ke dalam proses bisnis security operations organisasi. Salah satu metode untuk menggambarkan proses bisnis adalah dengan menggunakan Business Process Modelling & Notation (BPMN). CTI di BSSN menjadi tugas dari Subdirektorat Deteksi Potensi Ancaman (D143). D143 menjalankan CTI dengan mekanisme pelaporan dan distribusi informasi pada proses diseminasi atau dikenal dengan cyber threat information sharing yang berefek terhadap kinerja D143. Dalam penelitian ini dilakukan User Requirements Analysis dan perancangan proses bisnis cyber threat information sharing pada D143. Dari hasil analisis kebutuhan, akan dirancang rekayasa proses bisnis yang sesuai untuk D143 menggunakan notasi BPMN untuk menggambarkannya. Pengujian proses bisnis yang dirancang dilakukan dengan cara melakukan simulasi terhadap proses bisnis, serta validasi kesesuaian rancangan proses bisnis dengan kebutuhan D143. Hasil dari penelitian ini menunjukkan proses bisnis yang dirancang dapat dijalankan pada platform berbasis STIX dan TAXII, namun belum sepenuhnya terotomasi dalam melakukan proses cyber threat information sharing.

Kata kunci: proses bisnis (1), CTI (2), *cyber threat information sharing* (3), STIX dan TAXII (4), BPMN (5).

1. PENDAHULUAN

Ancaman yang berkembang dewasa ini membawa skenario yang jauh lebih kompleks, dimana kapabilitas serangan yang lebih maju dan jarang terjadi sebelumnya, menjadi hal yang sering ditemukan saat ini. Pihak penyerang (*adversary*) tidak semata-mata terfokus pada serangan yang tersebar luas dan bersifat merusak seperti pada *worm*, namun cenderung memiliki target yang diserang secara bertahap untuk mencapai tujuan tertentu dan juga berusaha untuk dapat memiliki akses yang berkelanjutan pada sistem target [1]. Pendekatan tradisional dalam keamanan siber yang berfokus pada penanganan kerentanan, sudah tidak cukup efektif, dikarenakan diperlukan adanya metode pertahanan yang proaktif untuk mengefektifkan pertahanan secara defensif [1]. Hal ini berarti bahwa akan selalu ada kerentanan yang terjadi akibat semakin bervariasinya teknik penyerangan dan tidak efektif apabila terus melakukan penanganan terhadap kerentanan yang terjadi. Postur keamanan yang efektif terhadap tren ancaman saat ini, membutuhkan pemahaman terhadap perilaku, kemampuan, dan niat dari *adversary* [1]. Artinya, dengan pemahaman yang seimbang antara pihak penyerang dan kondisi kita sendiri, kita dapat memahami tentang sifat dasar dari ancaman sehingga dapat mengambil langkah-langkah akurat untuk melakukan pertahanan yang baik.

Cyber Threat Intelligence (CTI) adalah sistem pengelolaan pengetahuan berbasis bukti, termasuk di dalamnya terdapat konteks, mekanisme, indikator, dan saran yang dapat ditindaklanjuti, tentang ancaman yang ada atau muncul terhadap aset, sehingga dapat digunakan untuk mengambil tindakan terhadap ancaman tersebut [2]. CTI memberikan informasi terkait potensi ancaman siber, sehingga organisasi dapat mengambil kebijakan stategis, operasional serta taktis untuk menghadapi ancaman yang dapat berpengaruh pada organisasi [3]. CTI dapat menjadi solusi dalam memberikan pemahaman terhadap kemampuan-kemampuan yang dimiliki oleh *adversary*.

CTI dapat dibagi menjadi 3 (tiga) bagian besar, pengumpulan informasi, analisis, serta pemanfaatan dan diseminasi [4]. Diseminasi bertujuan untuk menyebarkan informasi CTI, sehingga setiap *stakeholder* dapat mengetahui informasi tersebut. Proses ini dikenal dengan istilah *cyber threat information sharing* [5].

Dengan berkembangnya CTI, komunitas dan organisasi ikut serta dalam tren CTI ini. Khusus dalam proses diseminasi, Organization for the Advancement of Structured Information Standards (OASIS), suatu konsorsium yang mengembangkan standar untuk komunitas teknologi informasi secara global, merancang *Structured Threat Information Expression* (STIX) sebagai format untuk memetakan informasi CTI secara terstruktur [1]. Selain STIX, dikembangkan juga *Trusted Automated Exchange of Intelligence Information* (TAXII) yang merupakan protokol aplikasi yang berjalan pada *Hypertext Transfer Protocol Secure* (HTTPS) sebagai mekanisme pertukaran informasi CTI [6]. Dengan

adanya STIX dan TAXII, beberapa *platform* untuk *cyber threat information sharing* dikembangkan dengan berbasis STIX dan TAXII, seperti *Malware Information Sharing Platform* (MISP), AlienVault Open Threat eXchange (OTX), EclecticIQ, Anomali STAXX, Cabby, OpenTAXII, dan sebagainya.

CTI yang efektif adalah CTI yang dapat terintegrasi ke dalam proses bisnis *security operations* organisasi. Proses bisnis merupakan elemen utama fungsi bisnis di suatu organisasi yang melibatkan *stakeholder* dan membutuhkan sumber daya [7]. Sebuah proses bisnis dapat dijelaskan dengan sederhana sebagai aliran aktivitas kegiatan. Proses bisnis adalah kumpulan dari tugas atau aktivitas yang terstruktur yang dapat menghasilkan layanan atau produk tertentu untuk satu atau banyak konsumen [7]. Perancangan proses bisnis merupakan bagian dari siklus proses bisnis [8]. Dalam siklus proses bisnis tersebut, proses bisnis akan dirancang, dianalisis, diimplementasikan, dan dievaluasi. Untuk merancang proses bisnis, dibutuhkan penggambaran proses bisnis dengan tujuan lebih mudah untuk dipahami. Salah satu metode untuk menggambarkan proses bisnis adalah dengan menggunakan *Business Process Modelling & Notation* (BPMN).

Badan Siber dan Sandi Negara (BSSN) menjalankan CTI pada Subdirektorat Deteksi Potensi Ancaman (D143), Direktorat Deteksi Ancaman, Deputi Identifikasi dan Deteksi, menurut hasil wawancara. Berdasarkan hasil wawancara juga, D143 dalam menjalankan tugasnya untuk mendeteksi potensi ancaman siber, menjalankan CTI dengan mekanisme pelaporan dan distribusi informasi pada proses diseminasi. Dalam proses diseminasi tersebut, sebuah dokumen disusun oleh jajaran D143 yang berisi analisis, rekomendasi, serta *Indicator of Compromise* (IOC) terkait serangan siber, *malware*, maupun informasi mengenai aktor dari suatu serangan siber, dan kemudian dikirimkan kepada *stakeholder* tujuan. Bentuk-bentuk informasi yang terdapat pada dokumen tersebut antara lain, rekomendasi, analisis *tactics, techniques, and procedures* (TTP), alamat IP, hash file, dan nama domain.

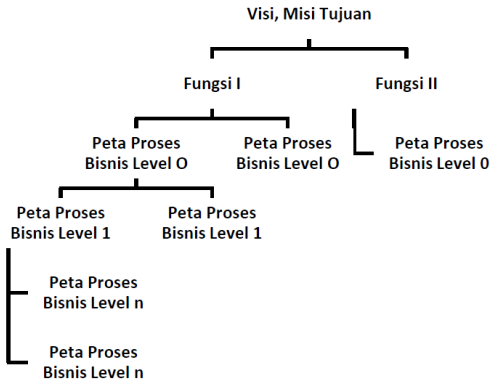
Permasalahan timbul ketika D143 menggunakan mekanisme tersebut pada proses *cyber threat information sharing*. Dengan proses bisnis yang dijalankan secara manual, terdapat beberapa kekurangan yaitu waktu yang lebih lama, tidak efisien terhadap perubahan proses bisnis, rentan terhadap *error* dan inkonsistensi data, serta bergantungnya pada penggunaan kertas [9]. Dikarenakan D143 masih menggunakan mekanisme tersebut, sehingga beberapa masalah yang diidentifikasi dari hasil wawancara adalah waktu dan efisiensi serta inkonsistensi data, yang pada akhirnya berefek terhadap kinerja D143.

Pada penelitian ini akan dilakukan *User Requirements Analysis* dan perancangan proses bisnis *cyber threat information sharing* dengan memanfaatkan *platform* berbasis STIX dan TAXII sehingga D143 dapat lebih efisien dan efektif dalam menjalankan tugas dan fungsinya. Selain itu, BPMN juga digunakan untuk menggambarkan proses bisnis yang telah dirancang.

2. LANDASAN TEORI

2.1. Perancangan dan Analisis Proses Bisnis

Untuk perancangan proses bisnis pada lingkungan instansi pemerintah, terdapat dokumen Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 19 Tahun 2018 [10]. Pada Bab III Peraturan Menteri tersebut, dijelaskan mengenai penyusunan peta proses bisnis menggunakan level atau tingkatan. Kerangka peta proses bisnis dengan level atau tingkatan digambarkan pada Gambar 1. Peta proses bisnis yang dimiliki instansi pemerintah, berdasarkan tingkatannya dimulai dari peta proses bisnis level 0, level 1, sampai dengan peta proses bisnis level ke n, dapat dijelaskan pada Gambar 1:



Gambar 1. Kerangka Peta Proses Bisnis Menggunakan Level atau Tingkatan [10]

2.2. *Cyber Threat Intelligence*

Cyber Threat Intelligence (CTI) adalah pengetahuan berbasis bukti, termasuk di dalamnya terdapat konteks, mekanisme, indikator, dan saran yang dapat ditindaklanjuti, tentang ancaman yang ada atau muncul terhadap aset, sehingga dapat digunakan untuk mengambil tindakan terhadap ancaman tersebut [2]. CTI memberikan informasi terkait potensi ancaman siber, sehingga organisasi dapat mengambil kebijakan stategis, operasional serta taktis untuk menghadapi ancaman yang dapat berpengaruh pada organisasi [3].

2.3. *Cyber Threat Information Sharing*

Cyber threat information adalah setiap informasi yang dapat membantu organisasi mengidentifikasi, menilai, memantau, dan merespons ancaman siber. *Cyber threat information* mencakup indikator; taktik, teknik, dan prosedur (TTP) yang digunakan oleh penyerang; tindakan yang disarankan untuk mendeteksi, menilai, atau mencegah serangan; dan temuan-temuan dari hasil analisis insiden [11].

Organisasi yang berbagi informasi ancaman dunia maya dapat memperbaiki postur keamanan mereka sendiri dan juga organisasi lain.

Dengan *cyber threat information sharing*, organisasi dapat memanfaatkan pengetahuan, pengalaman, dan kemampuan dari organisasi lain untuk mendapatkan pemahaman yang lebih lengkap tentang ancaman yang mungkin dihadapi [5].

2.4. MISP

Malware Information Sharing Platform (MISP) merupakan sebuah *platform* untuk berbagi, menyimpan, dan menghubungkan IOC dari suatu serangan, dan juga informasi ancaman siber lainnya [12]. *Platform* ini menyediakan *database* indikator, termasuk informasi teknis dan umum tentang informasi ancaman siber. Data-data tersebut disimpan dalam format terstruktur dan dengan model data yang fleksibel sehingga dapat menjelaskan relasi antar data [13].

2.5. STIX

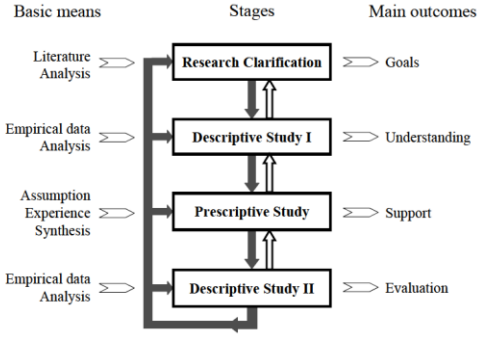
Structured Threat Information Expression (STIX) merupakan format untuk memetakan informasi CTI secara terstruktur. STIX mendukung proses manajemen *cyber threat information* yang lebih efektif, terstruktur, dan terotomasi [1].

2.6. TAXII

The Trusted Automated eXchange of Indicator Information (TAXII) merupakan protokol aplikasi yang berjalan pada Hypertext Transfer Protocol Secure (HTTPS) sebagai mekanisme pertukaran informasi CTI [6]. TAXII sangat fleksibel sehingga mendukung berbagai *sharing model*, memiliki komunitas yang aktif, serta merupakan standar yang diakui secara internasional.

3. METODE PENELITIAN

DRM terdiri dari 4 tahapan, yaitu *Research Clarification* (RC), *Descriptive Study* I (DS-I), *Prescriptive Study* (PS), dan *Descriptive Study* II (DS-II). Tahapan DRM digambarkan pada Gambar 2. Panah dengan cetak tebal antar tahapan menggambarkan aliran proses utama, dan panah dengan cetak tipis menggambarkan iterasi. Pada penelitian ini keempat tahapan akan digunakan.



Gambar 2. Tahapan DRM [14]

Langkah-langkah penelitian yang dijabarkan dari tahapan DRM adalah:

a. Melakukan studi literatur terkait perancangan proses bisnis, BPMN, CTI, *cyber threat information sharing*, STIX, dan TAXII.
b. Melakukan *User Requirements Analysis* untuk mengetahui spesifikasi kebutuhan *cyber threat information sharing* dari D143.
c. Merancang proses bisnis *cyber threat information sharing* berdasarkan hasil studi literatur dan *User Requirements Analysis* dengan notasi BPMN.
d. Melakukan uji fungsional terhadap proses bisnis yang dirancang. Uji fungsional dilakukan dengan instalasi dan konfigurasi *platform* yang telah ditentukan, mengubah laporan CTI menjadi format STIX, serta melakukan impor ke dalam *platform*.
e. Melakukan validasi dari hasil penelitian untuk mewujudkan tujuan penelitian dengan melakukan analisis dari hasil uji fungsional dan validasi ke lokus penelitian.

Objek dari penelitian ini adalah proses *cyber threat information sharing* yang dijalankan oleh Subdirektorat Deteksi Potensi Ancaman (D143) Badan Siber dan Sandi Negara sebagai lokus penelitian.

4. HASIL DAN PEMBAHASAN

4.1. *User Requirements Analysis*

4.1.1. *Information Gathering*

Pada penelitian ini, observasi dilakukan terhadap kegiatan operasional CTI yang dilakukan oleh jajaran D143, yaitu pada proses pengumpulan data, pembuatan laporan CTI, serta proses diseminasi. Observasi dilakukan pada Oktober tahun 2019. Terdapat beberapa hal yang diamati dari operasional tersebut, yaitu:

a) Beberapa kegiatan operasional masih dilakukan manual, seperti pengumpulan data dari CTI *feed*, pembuatan laporan CTI, dan diseminasi laporan CTI ke unit kerja ataupun instansi lain.
b) Laporan CTI dibuat berdasarkan arahan dari pimpinan D143.

4.1.2. *User Needs Identification*

Dari hasil wawancara dengan narasumber dari Subdirektorat Deteksi Potensi Ancaman, diidentifikasi beberapa kebutuhan dalam *cyber threat information sharing*, yaitu:

a) Proses *cyber threat information sharing* dapat menggunakan *platform-platform* yang sudah dikembangkan oleh pihak lain.
b) *Platform* yang digunakan berbasis STIX dan TAXII yang telah banyak diadopsi oleh banyak pengembang *platform*.

c) Beberapa *tagging* atau STIX *object* yang diperlukan oleh lokus penelitian adalah, jenis *malware*, *Common Vulnerabilities and Exposures* (CVE), pola serangan berdasarkan MITRE ATT&CK, serta alias dari aktor serangan. Diperlukan juga adanya pembagian sektor diseminasi, misalnya pengelompokan instansi-instansi yang bergerak pada bidang kesehatan. Apabila memungkinkan, digunakan *platform* yang mendukung adanya relasi antar satu informasi dan yang lainnya.

4.1.3. *Envisioning and Evaluation*

Dari hasil *Information Gathering* dan *User Needs Identification* disimpulkan skema awal untuk proses bisnis *cyber threat information sharing* seperti pada Gambar 3. Data dari berbagai sumber mengenai *cyber threat information*, dikumpulkan oleh Staf D143. Setelah data terkumpul, Staf D143 melakukan analisis terhadap data tersebut dan membuat laporan CTI. Setelah laporan CTI tersebut disetujui oleh Kepala Subdirektorat D143, laporan tersebut kemudian didesiminasi melalui *cyber threat information sharing platform*. Sebelum dilakukan penggunaan *platform* ini, dilakukan pemilihan *platform*.

Gambar 3. Skema awal proses bisnis *cyber threat information sharing*

4.1.4. *Requirements Specification*

Setelah adanya skema awal proses bisnis *cyber threat information sharing* seperti pada Gambar 3, kemudian dirancang spesifikasi dari kebutuhan lokus penelitian. Spesifikasi kebutuhan tersebut adalah:

a) Peran jajaran D143 masih diperlukan dalam pengumpulan data secara manual, serta pembuatan laporan CTI.
b) *Platform* yang digunakan berbasis STIX dan TAXII. Sebelum *platform* digunakan, dilakukan pemilihan *platform* terlebih dahulu.
c) STIX *object* yang diperlukan oleh lokus penelitian adalah *tag* pembagian sektor setiap informasi, jenis *malware*, *Common Vulnerabilities and Exposures* (CVE), motif serangan, serta alias dari aktor serangan. Apabila memungkinkan, digunakan *platform* yang mendukung adanya relasi antar satu informasi dan yang lainnya.

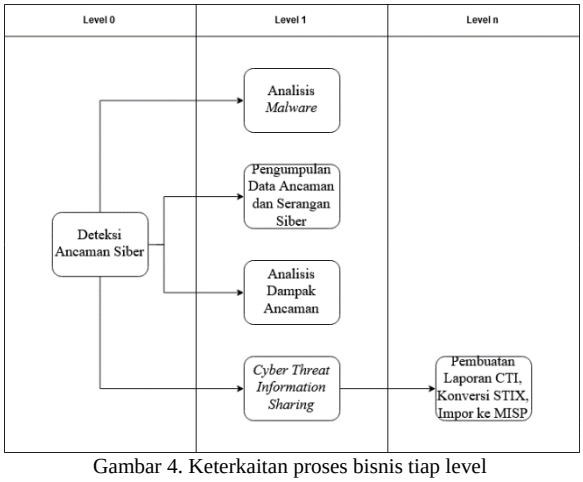
4.2. Perancangan Proses Bisnis

4.2.1. Pemilihan *Platform*

Berdasarkan spesifikasi kebutuhan yang dilakukan, peneliti menyimpulkan bahwa *platform* yang sesuai untuk kebutuhan dari lokus penelitian adalah *platform* yang berbentuk sebuah *portal information sharing*. Berdasarkan analisis kebutuhan, digunakan MISP dengan alasan *platform* tersebut telah digunakan oleh BSSN, sehingga D143 tidak perlu lagi melakukan instalasi serta konfigurasi *platform* lain dalam proses *cyber threat information sharing*. Selain dari alasan tersebut, MISP merupakan salah satu *platform* yang paling lengkap serta fleksibel, yang mampu memetakan proses CTI secara keseluruhan [13]. MISP mampu menerima berbagai format untuk impor maupun ekspor data, seperti STIX, OpenIOC, CybOX, JSON, CSV, dan XML. Berdasarkan perbandingan antar *platform* CTI, MISP mampu diintegrasikan dengan *Intrusion Detection System* (IDS) maupun *Security Information and Event Management* (SIEM), disamping lengkap serta fleksibilitas yang diberikan oleh MISP [13].

4.2.2. Perancangan Proses Bisnis

Berdasarkan teknik perancangan proses bisnis pada instansi pemerintah [10], digunakan teknik perancangan menggunakan level atau tingkatan. Perancangan proses bisnis *cyber threat information sharing* berada pada perancangan proses bisnis level *n* berdasarkan dokumen tersebut. Gambar 4 memperlihatkan peta proses bisnis level 0, level 1, dan level *n* dari proses bisnis *cyber threat information sharing*. Dari tugas dan fungsi BSSN, diidentifikasi proses bisnis level 0 yang berkaitan dengan proses bisnis *cyber threat information sharing* adalah proses bisnis mengenai deteksi ancaman siber. Kemudian dari proses bisnis deteksi potensi ancaman siber yang berada pada level 0, terdapat proses bisnis level 1 yaitu proses bisnis yang berada pada ruang lingkup deteksi ancaman. Berdasarkan tugas dari Subdirektorat Deteksi Potensi Ancaman, diidentifikasi proses bisnis pada level 1 yang mendukung proses bisnis *cyber threat information sharing* adalah analisis *malware*, pengumpulan data ancaman dan serangan siber, serta analisis dampak ancaman.



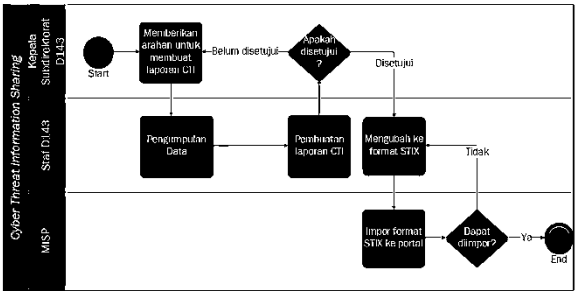
Gambar 4. Keterkaitan proses bisnis tiap level

Berdasarkan hasil *User Requirements Analysis* dan pemilihan *platform*, dirancang sebuah proses bisnis seperti pada Gambar 5.

Proses bisnis *cyber threat information sharing* yang dirancang, diawali dengan adanya arahan dari pimpinan untuk membuat laporan CTI dan melakukan

diseminasi terhadap laporan CTI tersebut. Kemudian Staf D143 melakukan pengumpulan data secara manual melalui berbagai sumber internal seperti Honeypot ataupun sumber eksternal berupa *feed* CTI yang digunakan oleh D143. Setelah mengumpulkan data, kemudian data tersebut dianalisis dan hasilnya dituangkan dalam sebuah laporan CTI. Laporan CTI ini berisi narasi, analisis, dan indikator terkait dengan topik yang diberikan.

Setelah laporan telah selesai dibuat, maka laporan tersebut kemudian diubah ke dalam format STIX, sehingga dapat diinput ke dalam portal MISP. Informasi-informasi yang dikonversi ke dalam format STIX berdasarkan dari spesifikasi kebutuhan. Konversi harus mengikuti aturan konversi setiap STIX *object*. Dalam portal MISP, informasi akan didiseminasi sesuai dengan tujuannya, apakah kepada seluruh komunitas dalam portal tersebut, maupun kepada suatu pihak tertentu saja. Setelah informasi sudah berada di portal MISP dan dapat diakses oleh pihak tujuan, maka diseminasi informasi sudah berjalan.



Gambar 5. Proses bisnis *cyber threat information sharing*

4.3. Instalasi dan Konfigurasi MISP

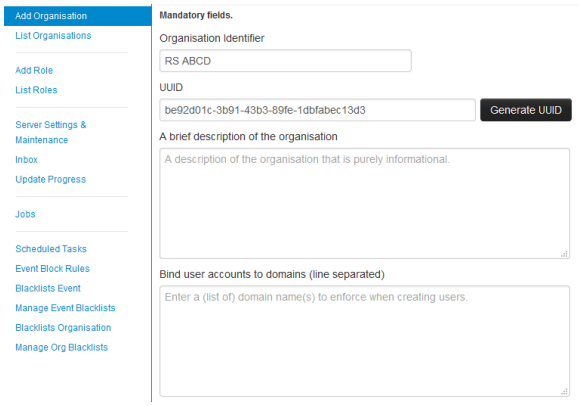
4.3.1. Mengunduh dan Menginstal ke dalam *Software* Virtualisasi

Dalam penelitian ini digunakan *software* VMware Workstation untuk menggunakan MISP. Bentuk *virtual machine* dari MISP dapat diunduh pada URL https://www.circl.lu/misp-images/latest/. Setelah file tersebut diunduh, kemudian dimasukkan ke dalam *virtual machine*, dan dijalankan.

4.3.2. Pembuatan Sektor Diseminasi Informasi

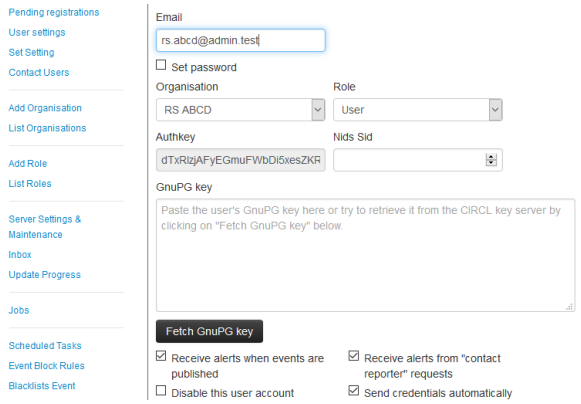
Salah satu kebutuhan lokus penelitian adalah adanya sektor diseminasi informasi. Artinya, adanya pengelompokan penerima informasi yang didiseminasi. Sebagai contoh, penerima dari sektor Infrastruktur Kritis Nasional di bidang Kesehatan adalah instansi-instansi dalam bidang tersebut seperti rumah sakit. Sektor kesehatan dipilih dikarenakan sektor ini merupakan sektor infrastruktur kritis nasional, dimana banyak instansi merupakan bagian dari sektor ini. Hal ini menyebabkan instansi-instansi dari sektor kesehatan ini yang menjadi target dari *adversary*. Untuk membuat sektor ini pada MISP, akan dibuat kelompok untuk sektor tersebut dan sebuah *user* dalam suatu instansi di sektor tersebut.

Untuk membuat akun dari suatu instansi, pada MISP terdapat menu "*Administration*", yang kemudian disorot dan dipilih submenu "*Add Organisations*". Gambar 6 menunjukkan informasi yang dimasukkan dalam pembuatan kelompok tersebut. Setelah informasi-informasi tersebut dimasukkan, lalu diselesaikan dengan menekan tombol "*Submit*".



Gambar 6. Membuat akun suatu instansi MISP

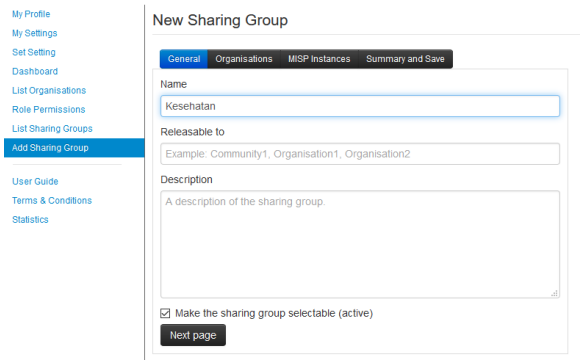
Untuk membuat akun dari *user* dalam instansi yang telah dibuat sebelumnya, dilakukan sorotan pada menu "*Administration*" dan dipilih pada submenu "*Add User*". Gambar 7 menunjukkan informasi yang dimasukkan saat membuat *user* untuk suatu instansi.



Gambar 7. Membuat *user* salah satu instansi dalam sektor kesehatan pada MISP

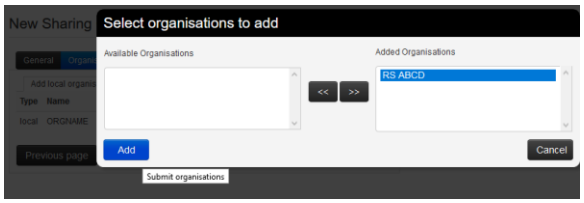
Terdapat kredensial yang dimasukkan seperti alamat email serta kata sandi. Kemudian pada opsi "*Organisation*", dipilih akun instansi yang telah dibuat sebelumnya. Setelah selesai, dipilih tombol "*Submit*".

Setelah membuat *user*, kemudian dibuat kelompok *sharing*. Untuk membuat kelompok tersebut, dilakukan sorotan pada menu "*Global Actions*", lalu dipilih submenu "*Add Sharing Group*". Pada *tab* "*General*" dimasukkan nama kelompok *sharing* seperti pada Gambar 8 setelah itu dipilih pada tombol "*Next Page*".



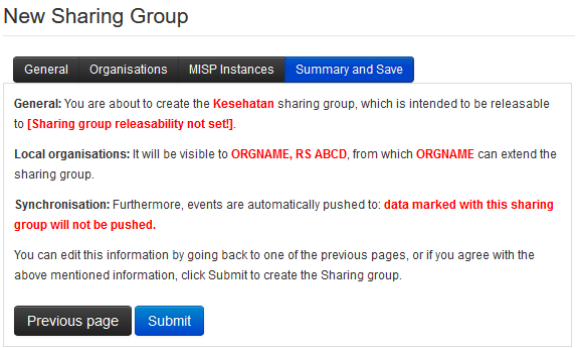
Gambar 8. *Tab* "*General*" dalam pembuatan kelompok *sharing* di MISP

Selanjutnya akan dialihkan ke *tab* "*Organisations*". Kemudian dipilih pada opsi "*Add local organization*", dan dipilih organisasi yang telah dibuat sebelumnya seperti pada Gambar 9. Selanjutnya dipilih tombol "*Next Page*" untuk melanjutkan proses.



Gambar 9. *Tab* pembuatan kelompok *sharing* di MISP

Setelah itu pada *tab* "*Summary and Save*" dipilih tombol "*Submit*" untuk menyelesaikan pembuatan kelompok *sharing* seperti pada Gambar 10.



Gambar 10. *Tab* "*Summary and Save*" dalam pembuatan kelompok *sharing* di MISP

4.4. Konversi ke Format STIX

Untuk melakukan konversi ke format STIX, digunakan informasi dari serangan WannaCry *ransomware* dan TrickBot *trojan* berdasarkan STIX *object* yang diperlukan oleh lokus, sebagai berikut:

I. WannaCry *ransomware*:
   a) Nama *malware*: WannaCry
   b) MD5 hash: db349b97c37d22f5ea1d1841e3c89eb4
   c) CVE: CVE-2017-0144
   d) MITRE ATT&CK *attack pattern*: *Data Encrypted for Impact*
   e) Aktor terduga: Lazarus *Group*

II. TrickBot trojan:
   a) Nama *malware*: TrickBot
   b) MD5 hash: f26649fc31ede7594b18f8cd7cdbbc15
   c) CVE: CVE-2017-0147
   d) MITRE ATT&CK *attack pattern*: *Masquerading*
   e) Aktor terduga: TA505

4.4.1. Konversi Identifier

Aturan dalam format STIX untuk *identifier* adalah menggunakan *universally unique identifier* versi 4 (UUIDv4). Untuk mendapatkan UUIDv4 digunakan *online generator* yang dapat diakses pada URL https://www.uuidgenerator.net/version4. Setelah membuka URL tersebut, UUIDv4 akan langsung tersedia seperti pada Gambar 11. Apabila ingin menggunakan UUIDv4 lainnya, dapat dilakukan pemuatan ulang pada laman web.

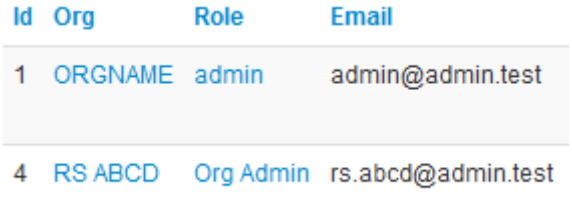
Gambar 11. UUIDv4 yang disediakan dari https://www.uuidgenerator.net/version4

4.4.2. Konversi Informasi menjadi format STIX

Seluruh informasi kemudian dikonversi ke dalam format STIX, untuk selanjutnya dilakukan impor ke dalam MISP.

4.5. Impor Format STIX ke MISP

Dalam tahapan ini, akun *default* dari instalasi MISP, yaitu akun "admin@admin.test" yang berada dalam instansi "ORGNAME" akan disimulasikan menjadi akun dari Staf D143, serta dengan tujuan diseminasi informasi kepada sektor kesehatan yang mana telah terdapat instansi "RS ABCD" dengan akun "rs.abcd@admin.test" yang telah dibuat sebelumnya. Kedua akun ini beserta instansinya diperlihatkan pada Gambar 12.

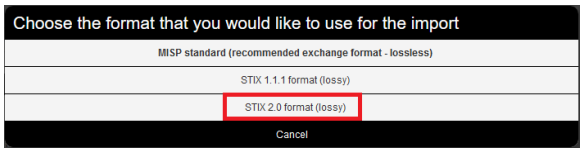


Gambar 12. Daftar organisasi serta *user*

Kedua instansi ini juga telah berada pada kelompok *sharing* yang sama, dimana telah dibuat serta dimasukkan ke dalam sektor kesehatan pada portal MISP tersebut.

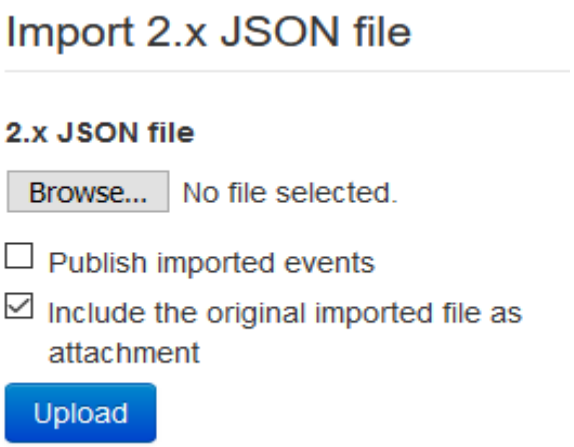
Format STIX kemudian diimpor ke dalam MISP. Pada simulasi ini, *user* "admin@admin.test" yang berperan sebagai Staf D143 melakukan impor format STIX ke dalam portal MISP dengan tujuan ke dalam

kelompok *sharing* sektor kesehatan. Untuk mengimpor format STIX tersebut, digunakan fitur "*Import from…*" pada tampilan awal MISP dan kemudian dipilih "*STIX 2.0 format* (*lossy*)" seperti pada Gambar 13.



Gambar 13. Impor format STIX ke dalam MISP

Kemudian akan dialihkan pada laman seperti pada Gambar 14. Pada laman ini, dipilih tombol "*Browse*" untuk memilih file format STIX yang telah digabungkan, dan dilakukan centang pada opsi "*Include the original imported file as attachment*" untuk menyertakan file format STIX tersebut di portal MISP nantinya. Opsi "*Publish imported events*" tidak dicentang agar *event* MISP tidak langsung dipublikasikan, hal inidikarenakan masih ada pengaturan lanjutan setelah melakukan impor. Setelah file dipilih, kemudian dipilih tombol "*Upload*".

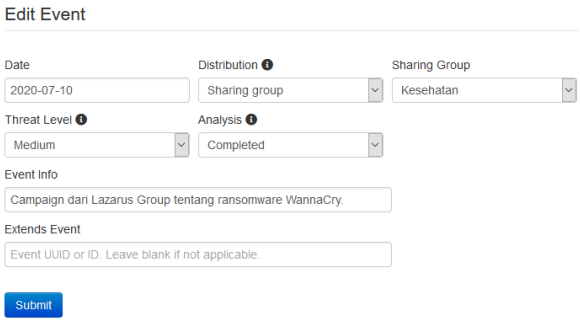


Gambar 14. *Import 2.x JSON file*

Setelah berhasil diimpor, akan muncul laman serta notifikasi seperti pada Gambar 15. Kemudian dilakukan pengaturan pada *event* yang telah diimpor ini, yaitu dengan memilih tombol "*Edit Event*" di sebelah kiri laman pada Gambar 15.

Gambar 15. Impor format STIX berhasil

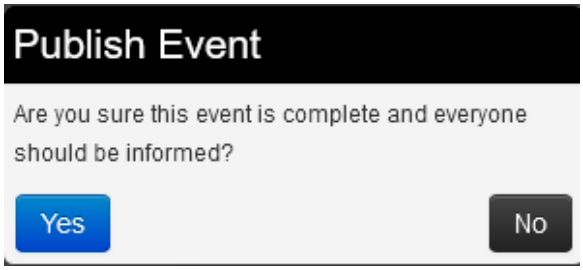
Kemudian akan ditampilkan laman "*Edit Event*" seperti pada Gambar 16. Pada opsi "*Distribution*" dipilih pilihan "*Sharing Group*" kemudian dipilih tujuan diseminasi yaitu kelompok *sharing* sektor Kesehatan. Pada opsi "*Threat Level*" dipilih pada pilihan "*Medium*" dikarenakan serangan WannaCry dan TrickBot merupakan serangan dari *malware* APT. Pada opsi "*Analysis*" dipilih pada pilihan "*Completed*" karena dianggap telah selesai dalam melakukan analisis serangan. Setelah selesai, pilih tombol "*Submit*".



Gambar 16. Laman "*Edit Event*"

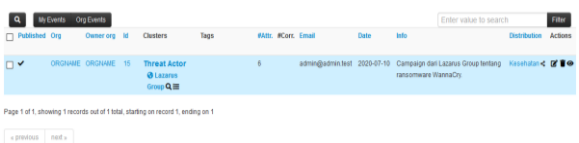
Pada opsi "*Threat Level*" dan "*Analysis*" sebenarnya adalah kebijakan dari yang melakukan impor format STIX dalam hal ini instansi D143. Sehingga pada kasus *real*, dapat disesuaikan dengan kondisi yang ada. Dalam simulasi ini, digunakan pilihan "*Medium*" pada opsi "*Threat Level*" serta pilihan "*Completed*" pada opsi "*Analysis*" untuk menjadi skenario dari penelitian ini.

Setelah dipilih tombol "*Submit*", akan kembali ke laman seperti pada Gambar 15. Langkah selanjutnya kemudian dilakukan publikasi dengan proses "*Publish Event*" yang berada pada kiri laman tersebut. Akan muncul jendela "*Publish Event*" seperti pada Gambar 17, dan dipilih tombol "*Yes*". Setelah itu akan kembali ke laman seperti pada Gambar 15.



Gambar 17. Jendela "*Publish Event*"

Setelah itu, dilakukan *login* ke dalam akun "RS ABCD", dan pada laman utama MISP, sudah terdapat *event* yang dipublikasikan pada portal MISP seperti pada Gambar 18.

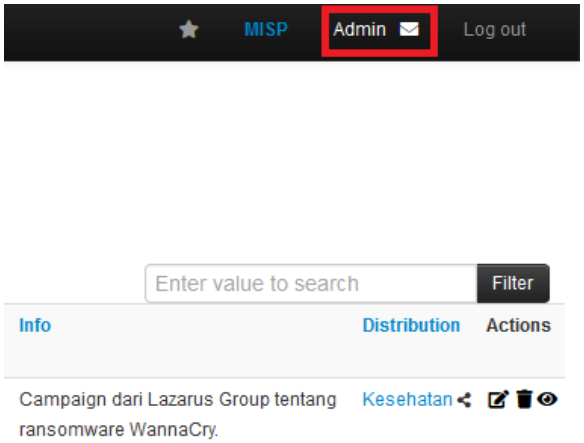


Gambar 18. *Event* telah dipublikasikan ke sektor kesehatan

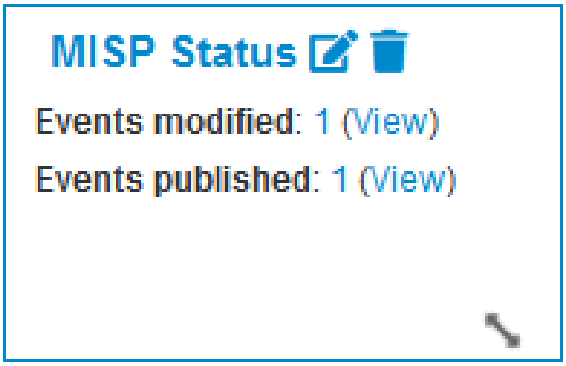
Apabila *event* tersebut dibuka, maka akan terdapat informasi-informasi yang sebelumnya telah diubah dalam format STIX. Informasi-informasi tersebut diperlihatkan pada Gambar 19.

Gambar 19. Informasi dari format STIX sudah dipublikasikan ke portal MISP

Terdapat juga notifikasi yang dapat dibuka pada laman utama MISP seperti pada Gambar 21. Notifikasi ini dapat digunakan apabila terdapat *event* baru yang ditambahkan ke dalam portal MISP. Apabila tombol notifikasi seperti pada Gambar 20 tersebut dibuka, maka akan terlihat notifikasi tentang *event* yang dimodifikasi ataupun yang baru saja dipublikasikan.



Gambar 20. Tombol notifikasi pada laman utama MISP



Gambar 21. Laman notifikasi pada MISP

4.6. Hasil Validasi

Validasi dilakukan dengan memberikan hasil penelitian serta melakukan diskusi dengan pihak lokus penelitian. Dari hasil validasi, lokus penelitian menyampaikan beberapa hal:

a. Hasil penelitian menunjukkan proses bisnis telah berhasil dirancang dan dilakukan uji fungsional pada proses konversi ke format STIX serta impor ke dalam MISP;
b. Spesifikasi kebutuhan STIX object dari lokus yaitu jenis *malware*, *Common Vulnerabilities and Exposures* (CVE), pola serangan berdasarkan MITRE ATT&CK, serta alias dari aktor serangan dapat dikonversi menjadi format STIX. Selain itu juga disimulasikan pembagian sektor diseminasi, dimana sektor Kesehatan digunakan sebagai contoh.
c. Penelitian ini memberikan efisiensi diseminasi informasi ke target tujuan, dengan menggunakan format STIX dan *platform* MISP. Otomasi diseminasi informasi belum dapat dilakukan pada penelitian ini.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa:

a. Penelitian berhasil dilakukan dengan tahapan-tahapan yang telah ditetapkan.
b. Pada hasil simulasi proses bisnis, informasi-informasi potensi ancaman siber dapat dikonversi menjadi format STIX dan berhasil diimpor ke dalam MISP. Diseminasi informasi berhasil dilakukan dengan menggunakan fitur *sharing group* pada MISP sesuai target tujuan.
c. Validasi dari lokus penelitian menyatakan bahwa proses bisnis yang dirancang sudah dapat berjalan dan telah menggunakan spesifikasi kebutuhan dari lokus. Pada penelitian ini belum terdapat otomasi diseminasi informasi pada proses bisnis yang dirancang.

Dari hasil penelitian ini, dapat dikembangkan penelitian mengenai otomasi diseminasi informasi menggunakan *cyber threat information platform* lainnya, seperti OpenCTI, dan sebagainya. Selain itu dapat juga dilakukan otomasi diseminasi informasi antar *platform* yang berbeda, misalnya MISP ke Open CTI ataupun sebaliknya. Penelitian dari segi proses bisnisnya pun dapat dikembangkan pada perancangan proses bisnis yang berfokus pada pengumpulan data sebagai input untuk pembuatan laporan CTI.

6. REFERENSI

[1] S. Barnum, "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)," *MITRE Corp. July*, pp. 1–20, 2014.
[2] R. McMillan, "Definition: Threat Intelligence," 2013. [Online]. Available: https://www.gartner.com/en/documents/2487216.
[3] CERT-UK and CISCP, "An Introduction to threat intelligence," *Searchsecurity Buyers Guid.*, 2016.

[4] N. Kim, B. Kim, S. Lee, H. Cho, and J. Park, "Design of a Cyber Threat Intelligence Framework," *Int. J. Innov. Res. Technol. Sci. Int. J. Innov. Res. Technol. Sci.* |, 2017.

[5] A. Zibak and A. Simpson, "Cyber threat information sharing: Perceived benefits and barriers," in *ACM International Conference Proceeding Series*, 2019.

[6] J. Connolly, M. Davidson, and C. Schmidt, "The Trusted Automated eXchange of Indicator Information (TAXII ™)," *MITRE Corp.*, pp. 1–10, 2014.

[7] S. K. Sari and A. Asniar, "Analisis Dan Pemodelan Proses Bisnis Prosedur Pelaksanaan Proyek Akhir Sebagai Alat Bantu Identifikasi Kebutuhan Sistem," *J. INFOTEL - Inform. Telekomun. Elektron.*, 2015.

[8] M. Weske, *Business Process Management*, Third. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019.

[9] Mindfield Insights, "Manual vs Automated Business Processes," 2018. [Online]. Available: https://mindfieldconsulting.com/manual-vs-automated-business-processes/. [Accessed: 30-Jun-2020].

[10] Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, *Penyusunan Peta Proses Bisnis Instansi Pemerintah*. 2018.

[11] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "NIST Special Publication - Guide to Cyber Threat Information Sharing," *NIST Special Publication*. 2016.

[12] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP - The design and implementation of a collaborative threat intelligence sharing platform," in *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, 2016.

[13] A. de Melo e Silva, J. J. C. Gondim, R. de Oliveira Albuquerque, and L. J. G. Villalba, "A methodology to evaluate standards and platforms within cyber threat intelligence," *Futur. Internet*, 2020.

[14] L. T. M. Blessing and A. Chakrabarti, *DRM, a design research methodology*. 2009.