Investigasi Insiden Kebocoran Data Menggunakan Integrasi Melalui Pendekatan *Open Source Intelligence* dan *Detection Maturity Level Model*

Dendi Risman Saputra[1)], Arizal Arizal[2)], Girinoto[3)]
(1) Badan Siber dan Sandi Negara, dendi.risman@bssn.go.id
(2) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, arizal@poltekssn.ac.id
(3) Rekayasa Perangkat Lunak Kriptografi, Politeknik Siber dan Sandi Negara, girinoto@poltekssn.ac.id

Abstrak

Kebocoran data terjadi karena sistem informasi mempunyai kerentanan yang dapat dieksploitasi dimana biasanya berasal dari kurangnya akan kesadaran keamanan informasi atau kesalahan mendasar dalam konfigurasi sistem. Ketika terjadi insiden kebocoran data, seringkali penyebab dan pelaku kejadian tidak diketahui sehingga diperlukan investigasi untuk mendapatkan informasi mengenai pelaku dan penyerangannya. Investigasi ini dapat dilakukan dengan menggunakan teknik Open Source Intelligence (OSINT). Dimana OSINT sendiri memiliki kelemahan pada aspek tidak ada suatu parameter atau hasil standar yang diperoleh. Sehingga pada penelitian ini mengusulkan suatu pendekatan integrasi aliran OSINT dengan Model Detection Maturity Level melalui simulasi investigasi pada salah satu kasus nyata jual beli data pribadi. Hasil dari penelitian ini mampu menghasilkan informasi mengenai pelaku atau pelaku kejadian kebocoran data tersebut. Hasil investigasi yang dilakukan dapat digunakan sebagai rekomendasi perbaikan sistem informasi sekaligus bermanfaat sebagai bukti untuk mendukung proses hukum.

Kata Kunci: investigasi, kebocoran data, OSINT, Model DML.

Abstract

Data leaks occur because information systems have vulnerabilities that can be exploited which usually originate from a lack of information security awareness or basic errors in system configuration. When a data leak incident occurs, often the cause and perpetrator of the incident are unknown so an investigation is needed to obtain information about the perpetrator and the attack. This investigation can be carried out using Open Source Intelligence (OSINT) techniques. Where OSINT itself has weaknesses in the aspect that there are no parameters or standard results obtained. So this research proposes an approach to integrating the OSINT flow with the Maturity Level Detection Model through a simulation investigation in a real case of buying and selling personal data. Where the results of this research are able to produce information regarding the perpetrator or perpetrators of the data leak incident. The results of the investigations carried out can be used as recommendations for improving the information system as well as being useful as evidence to support the legal process.

Keywords: data leaks, DML model, investigation, OSINT.

1. PENDAHULUAN

Suatu organisasi memerlukan sistem informasi digital untuk menyimpan, mengolah dan menyampaikan informasi kepada publik seperti penduduk dan konsumen dengan tujuan supaya organisasi tersebut dapat dengan mudah dan cepat dalam menyebarkan informasi [1]. Di sisi lain, penggunaan sistem informasi memiliki risiko keamanan yang tinggi apabila tidak dikelola dengan baik [2]. Salah satu risiko yang dapat terjadi, yaitu insiden kebocoran data. Berdasarkan Data Breach Incident Report (DBIR) yang diterbitkan oleh Verizon disebutkan bahwa terjadi 5.258 kasus kebocoran data pada perusahaan-perusahaan di dunia [3]. Hal tersebut semakin kuat dengan adanya laporan dari The International Criminal Police Organization (INTERPOL) dalam dokumen ASEAN Cyberthreat Assesment 2021. Laporan tersebut menyatakan bahwa banyak serangan siber seperti *phishing*, *malware*, *cyberscam* yang diarahkan kepada organisasi kesehatan, *e-commerce*, *social media*, situs pemerintahan atau perusahaan yang mengakibatkan kerugian besar bagi organisasi maupun konsumen. Salah satu kerugian yang terjadi adalah penyalahgunaan data pribadi akibat kebocoran data yang telah tersebar luas secara terbuka di dunia maya. Contoh kasus dalam laporan tersebut adalah insiden kebocoran data pada *e-commerce* asal Indonesia yaitu, Tokopedia dengan total data pengguna yang tersebar sebanyak 91 juta akun [4].

Ketika insiden kebocoran data terjadi disebabkan karena memiliki banyak kemungkinan *attack vectors*. Dalam laporan Cost of a Data Breach Report 2021 yang disusun oleh International Business Machines (IBM), terdapat 10 *attack vectors* yang digunakan penyerang dalam mendapat data dari sebuah perusahaan meliputi *compromised credentials* (20%), *phishing* (17%), *cloud misconfiguration* (15%), *vulnerability in third-party software* (14%), *physical security compromise* (9%), *malicious insider* (8%), *accidental data loss/lost device* (6%), *system error*

(5%), *business email* (4)%, dan *social engineering* (2%) [5]. Ketika insiden kebocoran data telah terjadi, sering kali *attack vectors* serta identitas pelaku tidak diketahui sehingga diperlukan investigasi untuk memperoleh informasi seputar pelaku dan serangannya [5].

Investigasi terhadap insiden kebocoran data dapat menjadi dasar untuk menentukan perbaikan sistem informasi dalam mengurangi kemungkinan insiden yang sama terulang kembali di masa yang akan datang. Secara spesifik, investigasi merupakan penyelidikan dengan cara mencatat atau merekam fakta dengan melakukan peninjauan dan percobaan dengan tujuan untuk memperoleh jawaban [6]. Hasil dari investigasi dapat berupa data, informasi, serta jejak digital yang dapat digunakan untuk mendukung proses hukum [8].

Investigasi kebocoran data dapat dilakukan dengan menggunakan teknik *Open Source Intelligence* (OSINT) [6]. OSINT digunakan dengan memanfaatkan berbagai sumber terbuka yang dapat dijadikan acuan untuk mendapatkan informasi terkait identitas pelaku dan proses bagaimana pelaku kejahatan membocorkan data [6]. Data yang telah didapat kemudian akan dilakukan analisis untuk mendukung proses hukum bagi para pelaku serangan dan sebagai usulan perbaikan untuk meningkatkan keamanan sistem informasi [7] [8].

Pada penelitian yang dilakukan oleh Pastor-Galindo, *et al.* menjelaskan bahwa terdapat alur OSINT dapat diintegrasikan dengan *Detection Maturity Level* (DML) Model. Pada setiap proses DML berguna sebagai acuan dalam melakukan investigasi kejahatan siber [6]. DML Model merupakan *Cyberthreat Detection Scheme* yang merupakan parameter untuk mencari dan mengumpulkan informasi terkait identitas pelaku dan proses bagaimana pelaku melakukan serangan [5] [9]. DML merupakan model yang dapat diimplementasikan dalam OSINT karena memiliki kesamaan alur dengan OSINT [6]. Pada DML Model ini, tahapan yang dilakukan terdiri dari tiga tahap, tahapan pertama yaitu *host and network artifacts*, *atomic indicator*, *none or unknown* sebagai parameter untuk mendapatkan jejak yang tersimpan. Tahapan selanjutnya meliputi teknik, prosedur, *tools* untuk mengetahui bagaimana rencana dan metode eksekusi serangan. Tahapan terakhir yaitu *identity*, *goals*, *strategy* yang dapat digunakan untuk mencari tujuan dan profil penyerang.[10]. Sehingga pada penelitian ini, dilakukan simulasi OSINT yang diintegrasikan dengan DML Model dari penelitian Pastor-Galindo, *et al.* dengan objek insiden kebocoran data pada situs Raid Forum, yakni mengungkapkan aktor atau pelaku kebocoran data.

2. LANDASAN TEORI

2.1 Investigasi

Investigasi merupakan penyelidikan dengan cara mencatat atau merekam fakta dengan melakukan peninjauan dan percobaan, yang bertujuan untuk memperoleh jawaban atas pertanyaan atau hal yang dituju [11]. Hasil dari investigasi dapat berupa data jejak digital yang didapatkan dari hasil penelusuran yang akan mendukung proses hukum yang terjadi [8]. Pada saat insiden keamanan siber terjadi, investigasi penting dilakukan untuk mencari penyebab dari kemungkinan terjadinya insiden. Investigasi insiden keamanan siber dibutuhkan untuk mengetahui apa yang sebenarnya terjadi, meningkatkan kontrol, berbagi informasi dengan mitra bisnis, dan mencegah insiden terulang kembali di kemudian hari [11].

2.2 Kebocoran Data

Pada penelitian Nelson Novaes Neto, *et al* menyebutkan bahwa kebocoran data dapat didefinisikan sebagai sebuah insiden yang mengakibatkan tersebarnya *Personally Identifiable Information* (PII) yang berupa informasi elektronik [13]. PII merupakan segala informasi yang berkaitan dengan individu tertentu baik bersifat pribadi, publik, atau profesional. PII tidak hanya nama, alamat, dan informasi keuangan, tetapi meliputi hal yang bersifat individu lainnya seperti IP addresses, logon IDs, pengenal biometrik, data lokasi, rekaman video, riwayat konsumen, konten pribadi pada media sosial, dan foto [13] [14]

2.3 OSINT

Pada penelitian oleh Pastor-Galindo, *et al* menjelaskan bahwa banyak sekali informasi ataupun data yang dapat diperoleh dari teknik OSINT, mulai dari data biasa hingga data pribadi yang tersimpan secara terbuka di internet. OSINT berperan sebagai teknik untuk mengumpulkan informasi dari sumber internet [6]. Informasi yang diperoleh berasal dari riwayat dan tingkah laku pada akun media sosial atau forum, data yang diunggah atau tersimpan pada sistem informasi [8].

2.4 *Model Detection Maturity Level*

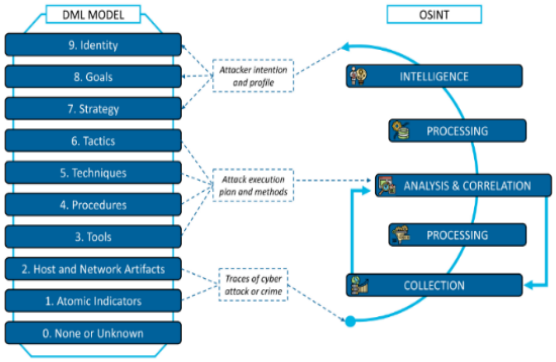
DML Model merupakan sebuah model deteksi dan respon ancaman serangan siber yang diusulkan oleh Ryan Stillions pada postingan blognya [15]. DML Model ini kemudian dikembangkan pada penelitian oleh Bromander, *et al.* [10] dengan menambahkan DML-9 -identify dan menambahkan presisi serta menggambarkan aspek kualitatif pada setiap tingkatannya. Pada penelitian lain yang dilakukan oleh Vasileios Mavroeidis, *et al.* menjelaskan bahwa DML juga dapat menjadi acuan untuk mendeteksi dan menangani serangan siber [16]. Level pada DML Model meliputi [10]: Tahapan pertama, DML 1 dan 2 yaitu *host* and *network artifacts*, *atomic indicator*, *none or unknown* sebagai parameter untuk mendapatkan jejak yang tersimpan. Tahapan selanjutnya, DML 3, 4, 5, dan 6 meliputi *techniques*, *procedures*, *tools* untuk mengetahui bagaimana rencana dan metode eksekusi serangan. Tahapan terakhir, DML 7,8, dan 9 yaitu *identity*,

goals, strategy yang dapat digunakan untuk mencari tujuan dan profil penyerang.[10].

3. METODE PENELITIAN

Objek penelitian ini adalah kasus insiden kebocoran data yang akan dilakukan investigasi dengan studi kasus nyata jual beli data pribadi pada situs Raid Forum [12].

Dimana secara umum tahapan dalam penelitian digambarkan pada Gambar 1.



Gambar 1. Tahapan penelitian

Pada alur OSINT ini, digunakan meliputi *Collection, Analysis & Correlation*, dan *Intelligence*. Selanjutnya, dilakukan identifikasi tingkat DML pada setiap alur OSINT tersebut. Setiap tingkat DML memiliki parameter jenis informasi yang menjadi target untuk didapatkan. Pada penelitian ini parameter DML bersumber dari penelitian DML yang dilakukan oleh Ryan Stillions [15] yang dikembangkan oleh Bromander, *et al*. [10]. Penggunaan alur DML disarankan untuk dilakukan berurutan mulai dari DML-1 hingga DML-9 dengan tujuan supaya hasil dari setiap tingkat DML terpenuhi. Apabila pada saat penelusuran informasi tidak dimulai dari DML awal maka akan mengakibatkan informasi pada DML awal tersebut tidak terpenuhi Parameter DML tersebut disajikan oleh penulis dalam bentuk tabel oleh penulis dengan menambahkan kode DML sebagai kode untuk mencari informasi tertentu yang dijelaskan pada Tabel 1, 2, dan 3.

Tabel 1.Parameter DML 1 dan 2

No	Target	Kode DML
1	Domain	DML-1A
2	IP Address	DML-1B
3	Nilai Hash File	DML-1C
4	Pola Serangan	DML-1D
5	Perilaku	DML-1E
6	IOC	DML-1F
7	File Tersimpan	DML-2A

Tabel 2. Parameter DML 3, 4, 5 dan 6

No	Target	Kode DML
1	Tools yang digunakan	DML-3A
2	Langkah serangan yang dilakukan	DML-4A
3	Metode untuk melakukan serangan	DML-5A
4	Taktik serangan yang dirancang dan dilakukan	DML-6A

Tabel 3. Parameter DML 7, 8 dan 9

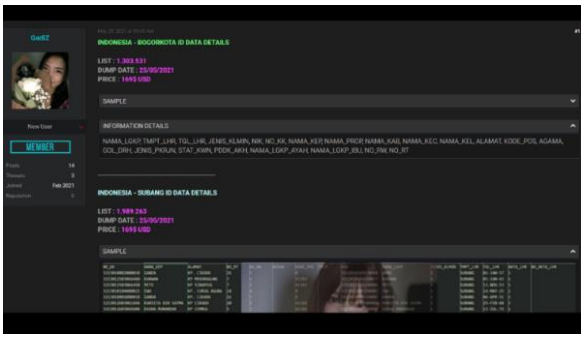
No	Target	Kode DML
1	Rencana serangan non-teknis	DML-7A
2	Pendekatan serangan non-teknis	DML-7B
3	Tujuan pelaku serangan	DML-8A
4	Motivasi pelaku melakukan serangan	DML-8B
5	Nama pelaku serangan	DML-9A
6	Organisasi pelaku serangan	DML-9B
7	Media Sosial pelaku serangan	DML-9C
8	Asal pelaku serangan	DML-9D

Bukti elektronik yang digunakan pada penelitian ini adalah perangkat virtual Android Virtual Device (AVD) dengan sistem operasi (OS) Android 12 *rooted*, Smartphone Google Pixel 3 XL yang menggunakan OS Android 12 *non-rooted*, dan OS Windows 11 yang disimulasikan dalam lingkungan virtual Vmware.

4. HASIL DAN PEMBAHASAN

4.1 Fase *Collection*

Pada bagian ini akan diberikan gambaran umum akan hasil pada observasi awal, akuisi dan koleksi informasi yang ditemukan. Dimana, pada Gambar 2, terdapat sebuah akun yang melakukan penjualan data pribadi yang berisi data penduduk Kota Bogor dengan jumlah 1.303.531 data dan Kabupaten Subang dengan jumlah 1.989.263 data. Pada laman tersebut juga akun dengan nama pengguna GadiZ memberikan informasi mengenai harga dari data pribadi dengan setiap harga data sebesar 169 USD. Selain jumlah dan harga, terdapat informasi tentang keterangan kapan data tersebut didapatkan, yaitu pada tanggal 25 Mei 2021.

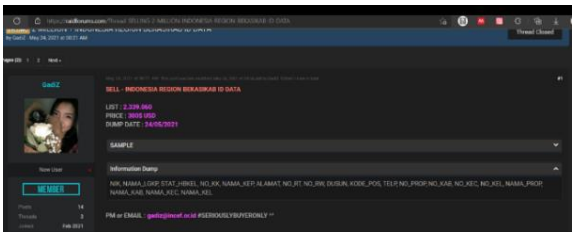


Gambar 2. Akun GadiZ melakukan penjualan data penduduk Kota Bogor dan Kabupaten Subang

Selanjutnya, pada Gambar 3, akun tersebut juga memberikan sampel terkait data pribadi yang didapatkan yang memuat kumpulan data pribadi yang bersifat sensitif dari penduduk yang seharusnya tidak terpublikasi.

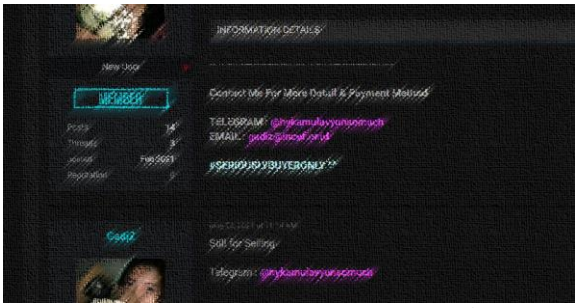
Selain pada postingan di atas, akun dengan nama pengguna GadiZ tersebut membuat postingan pada situs Raid Rorum [17] . Pada Gambar 4, terdapat informasi mengenai penjualan data pribadi penduduk Kabupaten Bekasi dengan mencantumkan harga 300 USD, jumlah data sebanyak 2.339.060 data dan waktu data itu didapatkan pada 24 Mei 2021.

Gambar 3. Sampel data dari Kota Bogor



Gambar 4. Aktifitas Akun GadiZ melakukan penjualan data Kabupaten Bekasi

Pada tahap *Acquisition*, dilakukan penelusuran metode OSINT dengan kata kunci yang didapatkan dari objek investigasi. Kata kunci tersebut merupakan informasi yang didapatkan dari tampilan laman pada objek investigasi. Selain dari laman utama, pada Gambar 5 ketika melakukan peninjauan lebih jauh pada kolom komentar akun GadiZ menyertakan informasi seputar *email* dan telegram yang dimiliki akun tersebut.

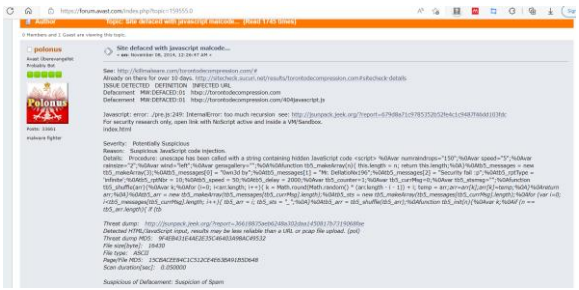


Gambar 5 Komentar akun GadiZ menyertakan informasi tambahan

Pada saat melakukan penelusuran lebih lanjut terdapat domain yang dapat dijadikan sumber utama yaitu didapati web Indonesia Cyber Freedom yang menjadi dugaan komunitas yang diikuti pelaku berdasarkan informasi dari *email* pelaku dengan domain dan IP incef.or.id seperti pada Gambar 6. Pada web tersebut tertulis beberapa nama pengguna yang diduga merupakan anggota dari komunitas atau forum tersebut.

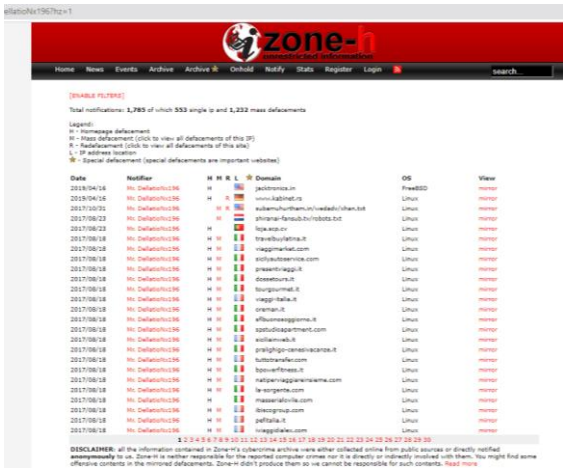
Gambar 6. Indonesia Cyber Freedom

Dalam situs lain seperti pada Gambar 7 ditemukan mengenai dugaan pola serangan yang berhubungan dengan *inject script* pada situs yang dijadikan target oleh pelaku penyerangan yang berdasarkan temuan pada forum Avast, yaitu terdapat dokumentasi serangan javascript *malicious code* oleh nama pengguna Mr.DellatioNx196. Nama Pengguna tersebut memiliki kesamaan dengan salah satu anggota yang ada pada situs incef.or.id sehingga diduga merupakan orang yang sama.



Gambar 7. Diskusi terkait serangan *defacement* oleh Mr. DellatioNx196

Selanjutnya nama pengguna Mr. DellatioNx196 ditelusuri menghasilkan riwayat *defacement* seperti pada Gambar 8 yang cukup banyak yang terdokumentasikan oleh Zone-H sehingga diduga memiliki perilaku sebagai *defacer*.



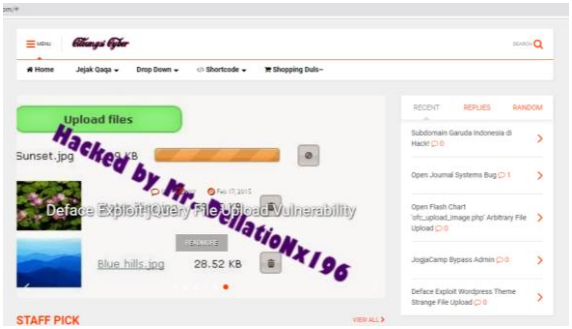
Gambar 8. Riwayat *defacement* oleh Mr. DellatioNx196 pada situs Zone-H

Selain dari situs Zone-H terdapat juga situs yang telah dilakukan *defacement* oleh Mr. DellatioNx196 yaitu seperti pada Gambar 9.

Gambar 9. Salah satu web yang mengalami *defacement* oleh Mr. DellatioNx196

4.2 Fase *Analysis & Correlation*

Penelusuran pada DML ini mencoba menelusuri bagaimana pelaku melakukan serangan, langkah-langkahnya serta *tools* yang digunakan. Pada Gambar 10 ditampilkan sebuah situs web dengan nama Cileungsi Cyber terdapat sebuah artikel yang mengindikasikan sebuah *tools* yang dibuat oleh Mr. DellatioNx196.



Gambar 10. Artikel terkait *tools defacement* yang dibuat oleh Mr. DellatioNx196

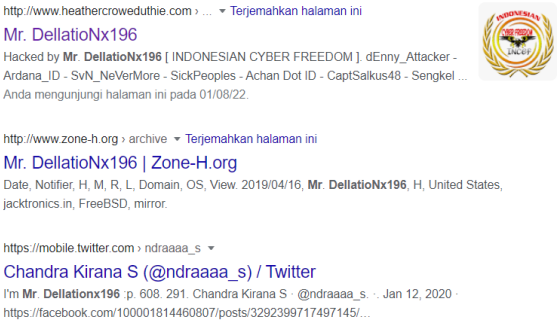
Pada situs tersebut juga terdapat kemungkinan *tools* lain dengan target *defacement* yang dijelaskan pada Gambar 11.

Gambar 11 Artikel terkait *tools defacement* kedua yang dibuat oleh Mr. DellatioNx196

Pada artikel yang ditulis pada halaman situs tersebut juga menampilkan bagaimana cara pemakaian *tools* tersebut seperti pada Gambar 12.

Gambar 12. Salah satu web yang mengalami defacement oleh Mr. DellatioNx196

Pada saat melakukan penelusuran pada situs Indonesia Cyber Freedom (INCEF) terdapat nama pengguna yang kemungkinan adalah nama anggota dari komunitas tersebut. Terdapat beberapa informasi menarik dari nama pengguna Mr.DellatioNx196 yang menjadi terduga pelaku utama pada kasus penjualan data pribadi yang dijelaskan dalam objek investigasi. Pada Gambar 13 menjelaskan bahwa setelah dilakukan penelusuran pada mesin pencari mengarah pada suatu nama yaitu MrXYX.

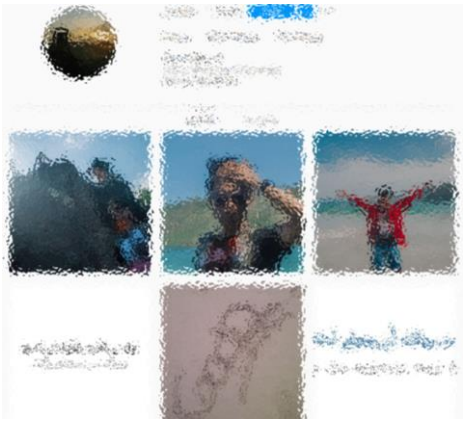


Gambar 13 Hasil penelusuran dengan *search engine*

Pada Gambar 14 terdapat akun media sosial twitter dengan nama pengguna @ndraaaa_s yang dalam artikelnya mengatakan bahwa akun tersebut merupakan Mr. DellatioNx196.

Gambar 14 *Akun Twitter MrXYX.*

Selanjutnya, terdapat alamat Cileungsi dan web incef.or.id yang berkaitan dengan informasi yang didapatkan pada tahap sebelumnya serta terdapat informasi email dengan nama ndrclz@outlook.jp. Kemudian terdapat informasi tambahan pada media sosial Instagram dengan kata kunci sama seperti nama email yaitu ndrclz ditemukan akun Instagram dengan nama MrXYX seperti pada Gambar 15.



Gambar 15 Akun Instagram MrXYX

Pada Gambar 16 terdapat artikel pada akun ndrclz menyinggung nama GadiZ yang merupakan nama pengguna aktor utama dalam objek investigasi. Pada situs lain yang merupakan situs project.co.id untuk mencari pekerjaan ditemukan kembali nama pengguna dan nama akun yang sama dengan Instagram dan Twitter pada Gambar 17.

Gambar 16 Postingan dari MrXYX yang menyebut nama GadiZ

Gambar 17 Akun Projects MrXYX

Berdasarkan informasi di atas dugaan menjadi semakin kuat bahwa pelaku jual beli data tersebut adalah MrXYX atau Mr. DellatioNx196 atau GadiZ, hal tersebut diperkuat dengan beberapa kali temuan pada artikel di media sosial dan di situsnya menyinggung nama-nama tersebut secara berkaitan.

Pada fase ini merupakan hasil yang didapatkan dari simulasi investigasi menggunakan integrasi OSINT dengan DML Model. Pada setiap tingkat DML berperan untuk menjadi acuan penelusuran informasi pada tingkat DML lain, apabila salah satu DML sebelumnya tidak mendapatkan informasi maka DML lainnya masih bisa mendapatkan informasi tanpa mengacu pada informasi di DML awal. Hal tersebut dikarenakan setiap tingkat DML dapat melakukan penelusuran informasi pada sumber terbuka secara mandiri menggunakan beragam platform yang dapat diakses melalui internet tanpa harus menunggu informasi dari DML lainnya. Akan tetapi, penggunaan DML sebagai parameter atau acuan harus dilakukan secara bertahap supaya informasi yang didapatkan saling berkaitan dan memenuhi setiap DML yang ada. Selanjutnya, hasil tersebut kemudian dimasukkan ke dalam beberapa tabel sebagai tabel ringkasan hasil sesuai dengan tahapannya. Sebagai ringkasan, berikut informasi awal yang didapatkan dan hasil dari simulasi pada setiap DML tersebut :

Dalam melakukan investigasi OSINT pasti terdapat informasi awal yang didapatkan dari sumber informasi pelaku utama, seperti pada kasus ini yaitu pada halaman akun tersebut di situs Raid Forum. Informasi awal akan berguna untuk menentukan arah dan tujuan ke mana investigasi selanjutnya dilakukan dengan mengacu pada DML Model. Pada investigasi ini mendapatkan beberapa hal penting untuk melanjutkan investigasi yaitu dijelaskan pada Tabel 4 yang merangkum informasi awal yang didapatkan pada situs Raid Forum.

Tabel 4 Informasi awal dari laman penjualan akun GadiZ

Jenis	Isi
Nama pengguna Akun Penjual	GadiZ
Akun Penjual pertama kali bergabung	Februari 2021
Email Penjual	gadiz@incef.or.id
Situs domain	incef.or.id
Akun Telegram	@hykamulavyuhsomuch

Informasi-informasi tersebut akan menentukan arah penelusuran informasi berikutnya dengan analisis yang dijelaskan Pada Tabel 5 sebagai berikut:

Tabel 5. Informasi awal dari laman penjualan akun GadiZ

Isi	Arah penelusuran informasi berikutnya
GadiZ	Dapat dilakukan pencarian pada platform media sosial atau forum untuk menemukan nama pengguna yang serupa ataupun menemukan informasi atau pembahasan yang membahas tentang akun dengan nama GadiZ.
Februari 2021	Waktu pertama kali bergabung pada Raid Forum akan berperan untuk menemukan dugaan informasi berikut: Keaktifan pelaku Kebenaran data pribadi Kemungkinan waktu data pribadi tersebut didapatkan.
gadiz@incef.or.id	Email dapat berperan untuk menemukan informasi mengenai asal ataupun situs asal pelaku
incef.or.id	Pada situs ini terdapat informasi yang menjelaskan sebuah komunitas Indonesia Cyber Freedom. Pada situs tersebut terdapat beberapa nama pengguna yang diduga merupakan daftar anggota komunitas tersebut. Oleh karena itu, daftar tersebut dapat dijadikan arah penelusuran informasi berikutnya karena dengan menelusuri daftar nama pengguna tersebut untuk mendapatkan informasi baru.
@hykamulavyuhsomuch	Akun tersebut dapat telusuri di telegram untuk menemukan tingkah laku dan informasi lainnya.

Informasi awal menjadi poin utama untuk melakukan investigasi selanjutnya. Tahapan selanjutnya adalah mencari informasi berdasarkan DML Model. Dalam penjelasan selanjutnya merupakan ringkasan hasil simulasi yang terdapat Kode DML, Keterangan, Sumber, dan Platform dengan penjelasan seperti pada Tabel 6.

Tabel 6 Penjelasan *Table Header*

Nama Table Header	Penjelasan
No	Sebagai urutan
Kode DML	Kode pengganti penjelasan parameter informasi yang dicari
Keterangan	Capaian informasi yang dicari dengan jawaban ada atau tidak.
Sumber	Asal-usul informasi didapatkan sehingga memenuhi sumber capaian pada DML. Sumber berupa Gambar pada sub bab Simulasi OSINT.
Platform	Media informasi atau Tools yang digunakan dalam menelusuri informasi

Tahapan pertama yaitu identifikasi pada DML-1 dan DML-2 pada tahap Collection menghasilkan informasi mengenai dugaan domain, IP address, pola serangan, dan perilaku dari pelaku. Oleh karena itu, pada tahap collection terdapat empat tingkat DML terpenuhi dari tujuh tingkat DML seperti yang dijelaskan pada Tabel 7.

Tabel 7 Ringkasan tahap Collection

No	Kode DML	Keterangan	Sumber	Platform
1	1A	Ada	Gambar 6	Situs Indonesia Cyber Freedom
2	1B	Ada	Gambar 6	Situs Indonesia Cyber Freedom
3	1C	Tidak ada	-	-
4	1D	Ada	Gambar 7	Forum Avast Security
5	1E	Ada	Gambar 8 dan 9	Situs Zone-h dan Situs Headercrowedguthie.com
6	1F	Tidak ada	-	-
7	2A	Tidak ada	-	-

Informasi pada identifikasi tingkat DML sebelumnya pada tahap collection berguna untuk penelusuran pada identifikasi DML pada tahap Analysis & Correlation. Pada tahap ini, ditemukan dugaan tools, Langkah, metode, dan taktik yang digunakan oleh pelaku. Dengan demikian, seluruh tingkat DML terpenuhi pada tahap ini seperti yang dijelaskan pada Tabel 8.

Tabel 8 Ringkasan tahap Analysis & Correlation

No	Kode DML	Keterangan	Sumber	Platform
1	3A	Ada	Gambar 10 dan 11	Situs Cileungsi Cyber
2	4A	Ada	Gambar 12	Situs Cileungsi Cyber
3	5A	Ada	Gambar 12	Situs Cileungsi Cyber
4	6A	Ada	Gambar 12	Situs Cileungsi Cyber

4.3 Fase Intelligence

Pada identifikasi DML di tahap Intelligence berdasarkan informasi yang ditemukan pada identifikasi di tahap Collection dan Analysis & Correlation. Pada identifikasi DML di tahap ini menemukan dugaan informasi meliputi tujuan, motivasi, nama, organisasi, media sosial, dan asal pelaku. Oleh karena itu, dari delapan tingkat DML pada tahap terdapat enam tingkat DML yang terpenuhi yang dirangkum pada Tabel 9.

Tabel 9 Ringkasan tahap Intelligence

No	Kode DML	Keterangan	Sumber	Platform
1	7A	Tidak ada	-	-
2	7B	Tidak ada	-	-
3	8A	Ada	Gambar 2	Situs Raid Forum
4	8B	Ada	Gambar 2 dan 17	Situs Raid Forum dan situs Projects
5	9A	Ada	Gambar 14, 15, 16 dan 17	Forum Twitter, Instagram, dan situs Projects
6	9B	Ada	Gambar 2, 6 dan 14	Situs Raid Forum, Situs Indonesia Cyber Freedom, dan Forum Twitter
7	9C	Ada	Gambar 4, 5, 14 dan 15	Situs Raid Forum, Situs Indonesia Cyber Freedom, dan Instagram
8	9D	Ada	Gambar 10 dan Gambar 14	Situs Cileungsi Cyber dan forum Twitter

5. KESIMPULAN

Simulasi investigasi yang dilakukan dengan menggunakan OSINT yang diintegrasikan dengan DML Model dapat digunakan untuk mengungkapkan identitas pelaku jual beli data pribadi. Setiap tingkat DML berperan sebagai parameter penelusuran informasi, bahkan setiap DML dapat saling membantu untuk mendapatkan informasi pada tingkat DML lainnya. Selanjutnya, hasil investigasi dari pelaku tersebut adalah pelaku dengan nama MrXYX atau Mr. DellatioNx196 atau GadiZ bertempat tinggal di Cileungsi, serta merupakan salah satu anggota dari komunitas Indonesia Cyber Freedom (INCEF). Pelaku tersebut aktif membuat dan menyebarkan *tools* serta *script* berbahaya dengan tujuan melakukan perusakan situs secara tidak bertanggung jawab. Dengan demikian, hasil investigasi tersebut dapat digunakan sebagai bukti tambahan untuk mendukung proses hukum dan peningkatan keamanan sistem informasi.

REFERENSI

[1] Cadelina Cassandra, Rudy, and Desi Maya Kristin, Website Quality Impact on Customers' Purchase Intention through Social Commerce Website

[2] N. Daswani and M. Elbayadi, "The Root Causes of Data Breaches," in Big Breaches, 2021. doi: 10.1007/978-1-4842-6655-7_1.

[3] "Verizon: Data Breach Investigations Report 2021," Computer Fraud & Security, 2021, doi: 10.1016/s1361-3723(20)30059-2.

[4] Interpol, "ASEAN Cyberthreat Assessment 2021 - Key Cyberthreat Trends Outlook From The Asean Cybercrime Operations Desk," 2021. Accessed: Nov. 25, 2021. [Online]. Available: https://www.interpol.int/content/download/

16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf
[5] IBM Security, "Cost of a Data Breach Report 2021," 2021. Accessed: Nov. 25, 2021. [Online]. Available: https://www.ibm.com/downloads/cas/OJDVQGRY
[6] J. Pastor-Galindo, P. Nespoli, F. G. Mármol, and G. M. Pérez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," IEEE Access, vol. 8, pp. 10282–10304, 2020, doi: 10.1109/ACCESS.2020.2965257.
[7] F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL," Information and Management, vol. 58, no. 1, 2021, doi: 10.1016/j.im.2020.103392.
[8] H. Williams and I. Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. 2018. doi: 10.7249/rr1964.
[9] K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws and controversies," in 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), 2016, pp. 1–9. doi: 10.1109/CyberSecPODS.2016.7502348.
[10] A. Jøsang and M. Eian, "Semantic Cyberthreat Modelling." STIDS, 2016.
[11] C. C. Chigozie-Okwum, D. O. Michael, and S. G. Ugboaja, "Computer forensics investigation; implications for improved cyber security in Nigeria," AFRREV STECH: An International Journal of Science and Technology, vol. 6, no. 1, pp. 59–73, 2017, doi: 10.4314/stech.v6i1.5.
[12] Indonesia - Bogorkota Id Data Details. (2022). diakses 19 April 2022, dari https://raidforums.com/Thread-SELLING-INDONESIA-SUBANG-BOGORKOTA-ID-DATA-DETAILS.
[13] N. N. Neto, S. Madnick, A. M. G. D. Paula, and N. M. Borges, "Developing a Global Data Breach Database and the Challenges Encountered," Journal of Data and Information Quality, vol. 13, no. 1, 2021, doi: 10.1145/3439873.
[14] "Data protection - European Commission." https://ec.europa.eu/info/law/law-topic/data-protection_en (accessed Nov. 26, 2021).
[15] "The DML model - Ryan Stillions." https://ryanstillions.blogspot.com/2014/04/tzhe-dml-model_21.html (accessed Nov. 26, 2021).
[16] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017, Dec. 2017, vol. 2017-January, pp. 91–98. doi: 10.1109/EISIC.2017.20.
[17] Sell - Indonesia Region Bekasikab Id Data. (2022). diakses 19 April 2022, dari https://raidforums.com/Thread-SELLING-2-MILLION-INDONESIA-REGION-BEKASIKAB-ID-DATA.