Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia

Adrian Admi[1], Abdul Hakim Nur Maulana[2]

[1,2]Pusat Operasi Keamanan Siber Nasional, Badan Siber dan Sandi Negara, Jakarta.
Email: [1]adrian.admi@bssn.go.id, [2]abdul.hakim@bssn.go.id

(Naskah masuk: 2 Juni 2020, diterima untuk diterbitkan: 9 Juni 2020)

ABSTRAK

Kemajuan Teknologi Informasi dan Komunikasi (TIK) membentuk suatu ruang siber yang memudahkan akses terhadap informasi dan pengelolaannya secara cepat dan akurat. Hal ini menyebabkan keamanan pada sistem dan informasi perlu untuk ditingkatkan, terutama pada sektor pemerintah yang menjadi target utama serangan siber. Data Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) BSSN pada tahun 2018 menunjukkan bahwa domain go.id menempati peringkat pertama dengan persentase 30,75% dengan mayoritas kasus web *defacement*. Secara umum memang banyak aspek yang harus diperbaiki terkait keamanan siber pada sektor pemerintah. Salah satu hal yang perlu ditingkatkan adalah koordinasi keamanan siber antar pemerintah pusat, instansi lain dan pemerintah daerah. Pada penelitian ini diberikan rekomendasi pola koordinasi keamanan siber antar instansi pemerintah dan alternatif solusi dari sisi teknologi dengan menerapkan teknologi *open-source*, salah satunya Elastic Stack. Elastic Stack dipilih karena mudah untuk dikembangkan sesuai kebutuhan dan kemampuan anggaran instansi pemerintah yang berbeda-beda, bersifat *open-source* yang didukung oleh komunitas sehingga dapat terus dikembangkan.

Kata kunci: *ancaman siber, keamanan siber, elastic stack, pemantauan jaringan.*

ABSTRACT

The advancement of Information and Communication Technology (ICT) forms a cyber space that facilitates access to information and its management quickly and accurately. This causes security in the system and information needs to be improved, especially in the government sector which is the main target of cyber-attacks. Data from the National Cyber Security Operations Center (Pusopskamsinas) of BSSN in 2018 showed that the go.id domain ranked first with a percentage of 30.75% with most web defacement cases. In general, there are indeed many aspects that need to be improved in relation to cyber security in the government sector. One thing that needs to be improved is the coordination of cyber security between the central government, other agencies, and local governments. In this study, recommendations are given for the pattern of cyber security coordination between government agencies and alternative solutions in terms of technology by applying open-source technology, one of which is Elastic Stack. Elastic Stack was chosen because it is easy to develop according to the needs and budget capabilities of different government agencies, which are open source supported by the community so that it can continue to be developed.

Keywords: *cyber threats, cyber security, elastic stack, network monitoring.*

1. PENDAHULUAN

Jaringan dan perangkat teknologi informasi dan komunikasi (TIK) semakin penting dalam kehidupan sehari-hari. Pada tahun 2016, hampir separuh dunia menggunakan internet, yaitu 3,5 miliar pengguna, dan menurut perkiraan, akan lebih dari 12 miliar perangkat yang terhubung ke internet pada tahun 2020. Di Indonesia, pengguna internet sudah mencapai 143,26 juta di tahun 2017 (APJII, 2018) dan menduduki urutan ke 4 tertinggi di dunia setelah India, China, dan Amerika Serikat (Hootsuite & We are social, 2019).

Penggunaan Internet ini telah mendorong Kemajuan Teknologi Informasi dan Komunikasi (TIK) dan telah membentuk suatu interkoneksi melalui internet yang menghubungkan berbagai sektor pemerintahan maupun bisnis dalam sebuah ruang siber (Chen dkk., 2004). Interkoneksi antar sektor dalam ruang siber membuat informasi menjadi mudah untuk diakses, diolah dan digunakan secara cepat dan akurat. Kemudahan akses informasi tentunya memberikan manfaat bagi organisasi karena informasi menjadi sumber daya penting yang membantu organisasi dalam pengambilan keputusan. Hal ini dirasakan semua negara, tak terkecuali juga di Indonesia.

Namun, semakin meningkatnya pemanfaatan TIK untuk pengelolaan informasi, maka semakin meningkat pula kebutuhan akan keamanan terhadap *database*, sistem, dan aplikasinya (Kumar dkk., 2005). Selain kebutuhan keamanan yang meningkat, kecenderungan risiko yang muncul juga meningkat sebagai konsekuensi dari kemudahan akses informasi (Hutchins dkk., 2015). Risiko yang dimaksud muncul dari ancaman maupun serangan siber berupa aktivitas *malware, data leakage and manipulation, web hacking incident, denial of service* (DoS) dan *distributed denial of service* (DDoS) (Kominfo, 2017).

Sektor yang menjadi perhatian adalah instansi pemerintah, karena menjadi target utama serangan siber. Hal ini dibuktikan dengan data dari Pusopskamsinas BSSN (Id-SIRTII, 2018) yang menyebutkan bahwa domain .go.id (*website* pemerintah) menempati peringkat pertama dengan 30,75% lebih sering terkena *defacement*, diikuti domain .ac.id dengan 28,38%, domain .sch.id dengan 12,58%, domain .co.id dengan 10,92%, dan domain .id dengan 8,25%. Data tersebut diperoleh dari Pemantauan *traffic* jaringan sejak awal Januari hingga akhir Desember 2018 dengan jumlah total sebanyak 16.939 insiden *website* (*defacement*).

Untuk memecahkan permasalahan tersebut, pertama, pemerintah harus membangun pola koordinasi antara pemerintah pusat dan pemerintah daerah. Salah satu cara untuk mengamankan sistem dan informasi adalah melakukan pengamanan pada infrastruktur jaringannya. Kemudian perlu juga dilakukan pemantauan terhadap infrastruktur jaringan instansi pemerintah untuk mendapatkan informasi tentang ancaman dan serangan yang keluar masuk ke jaringan serta data aktual terhadap kondisi terkini dari *host* atau *server* yang ada di jaringan. Hasil pemantauan juga dapat membantu instansi pemerintah dalam melakukan respon cepat terhadap insiden siber yang terjadi.

Dalam melakukan kegiatan pemantauan atau *monitoring* infrastruktur jaringan, dibutuhkan suatu sistem atau *tools* untuk membantu menemukan ancaman pada *traffic* jaringan dan *host*. Pilihan *tools/sensor monitoring* yang akan digunakan bisa beragam sesuai kondisi infrastruktur jaringan. Skema penerapan *tools* monitoring juga menjadi hal yang penting agar kegiatan *monitoring* dapat maksimal.

Dalam tulisan ini, Penulis merekomendasikan alternatif *tools* untuk memonitor *traffic* jaringan dan *host,* serta analisis log yang *free* (*open source*), *scalable* dan mudah untuk diimplementasikan pada instansi pemerintah yaitu Suricata, OSSEC, dan Elastic Stack (Elasticsearch, Logstash, Kibana).

Berdasarkan latar belakang yang telah disampaikan, maka permasalahan yang teridentifikasi adalah Bagaimana pola koordinasi keamanan siber antara pemerintah pusat dan pemerintah daerah? dan Bagaimana penerapan *monitoring traffic* jaringan dan *host* serta analisis log pada

infrastruktur jaringan menggunakan Suricata, OSSEC dan Elastic Stack?

Dalam tulisan ini, Penulis membatasi ruang ling-kup penelitian yaitu penerapan sensor dan analisis log dilakukan dalam skala laboratorium yang secara modular dapat diimplementasikan pada infrastruktur jaringan *data center* di instansi pemerintah.

Berdasarkan latar belakang, rumusan masalah dan pembatasan masalah, maka tujuan dan manfaat penelitian adalah memberikan gambaran tentang pola koordinasi antar instansi pemerintah dan penerapan sistem *monitoring* serta analisis *log* pada infrastruktur jaringan instansi pemerintah.

Kemudian manfaat penelitian adalah secara teoritis diharapkan dapat menjadi referensi bagi perkembangan fungsi keamanan siber guna mendukung pelaksanaan tugas instansi pemerintah dan menjaga ketahanan siber nasional. Manfaat Praktis diharapkan dapat memberikan masukan atau saran bagi BSSN dan instansi lain dalam melakukan penerapan *monitoring traffic* jaringan dan *host* serta analisis log pada suatu infrastruktur jaringan. Manfaat Kebijakan diharapkan dapat memberikan masukan kepada para pejabat di lingkungan BSSN dalam mengambil keputusan tentang kebijakan *monitoring traffic* dan *host* pada suatu infrastruktur jaringan.

2. METODOLOGI

Metodologi yang digunakan pada penelitian ini adalah simulasi yang merupakan bentuk penelitian yang bertujuan untuk mencari gambaran melalui sebuah sistem berskala kecil atau sederhana dimana di dalam model tersebut akan dilakukan manipulasi atau kontrol untuk melihat pengaruhnya. Penelitian ini mirip dengan penelitian eksperimental, perbedaannya adalah di dalam penelitian ini membutuhkan lingkungan yang benar-benar serupa dengan keadaan atau sistem yang asli.

3. HASIL DAN PEMBAHASAN

A. Pola Koordinasi, Pemantauan dan Respon Insiden

1. Pola Koordinasi dan Pemantauan

Badan Siber dan Sandi Negara (BSSN) adalah lembaga teknis non-kementerian yang didirikan pada 2017 berdasarkan Peraturan Presiden (Perpres) No. 133 tahun 2017 tentang Perubahan atas Perpres No. 53 tahun 2017 tentang Badan Siber dan Sandi Negara pada 16 Desember 2017 (Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara, 2017) (Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara, 2018). BSSN bukan merupakan lembaga baru yang dibentuk, namun merupakan revitalisasi Lembaga Sandi Negara (Lemsaneg) dengan tambahan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. Tugas utama BSSN adalah membangun ekosistem ranah siber Indonesia yang kuat dan aman, serta menjadi penyelenggara dan pembina persandian negara dalam menjamin keamanan informasi, utamanya yang berklasifikasi milik pemerintah atau negara, dengan tujuan untuk menjaga keamanan nasional.

Pada Gambar 3 dijabarkan mekanisme koordinasi BSSN dengan para pemangku kepentingan (Deputi Bidang Proteksi BSSN, 2018). Melalui dibentuknya *Security Operation Center* (SOC) (*information sharing and situational awareness*) di setiap instansi pemerintah pada dasarnya akan mempermudah dan mempercepat

terwujudnya keamanan siber secara menyeluruh, karena setiap pemangku kepentingan melakukan *monitoring* terhadap keamanan infrastruktur dan sistemnya masing-masing. Hal ini juga sesuai dengan keamanan siber jika dilihat dalam perspektif Undang-Undang Nomor 23 tahun 2014 tentang Pemerintah Daerah dan Peraturan Pemerintah Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Undang - Undang nomor 23 tahun 2014 tentang Pemerintah Daerah, 2012) (Peraturan Pemerintah Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, 2012).

Namun ada beberapa hal yang masih belum diputuskan dan menjadi tugas BSSN di masa depan untuk diselesaikan yaitu (Deputi Bidang Proteksi BSSN, 2018):

a. Konsep *multi-tiered* SOC.
b. Panduan untuk menentukan apakah setiap Kementerian dan Lembaga (K/L) atau Pemerintah Daerah perlu membangun SOC atau cukup menggunakan *Managed Service Security Provider* (MSSP) SOC.
c. Panduan untuk membangun, mengoperasikan dan tata kelola SOC.
d. Interoperabilitas SOC.
e. *Information sharing* antar SOC.

Untuk menjawab pertanyaan mengenai Interoperabilitas SOC, dalam penelitian ini dilakukan simulasi penerapan Elastic Stack sebagai pilihan alternatif *tools* untuk memantau *traffic* jaringan dan *host,* serta analisis log. Elastic Stack dipilih karena memiliki beberapa kelebihan, kemudian juga direkomendasikan oleh Adrian Grigorof pada *Open Source*/*Free Security Controls* (Grigorof, 2019).

2. Pola Respon Insiden

Dalam melakukan respon insiden, diperlukan personil, proses dan teknologi yang mendukung. Jika dalam suatu insiden siber di pemerintah daerah/instansi membutuhkan bantuan dari instansi lain maupun instansi pusat, dalam hal ini BSSN, diperlukan pola koordinasi yang tepat dan berjenjang agar tindakan respon insiden berjalan dengan efektif dan efisien. Pada Gambar 4 dijelaskan tentang Pola koordinasi respon insiden yang dirancang oleh Peneliti memanfaatkan struktur organisasi pemerintah daerah dan mengikuti konsep *multi-tiered* SOC yang ada.

Jika terjadi insiden siber pada level pemerintah daerah (Kabupaten/Kota) maka dengan bantuan teknologi monitoring yang ada (*firewall*, NIDS, HIDS, *log collection*), pemerintah daerah dapat melakukan respon insiden secara mandiri. Dalam prosesnya pemerintah Kabupaten/Kota dapat berkoordinasi terlebih dahulu dengan Pemerintah Provinsi, atau dapat juga langsung menghubungi BSSN melalui Pusopskamsinas. Dalam tulisan ini Penulis lebih merekomendasikan penyelesaian insiden siber yang dilakukan terlebih dahulu oleh Pemerintah Kabupaten/Kota hingga level Provinsi, untuk meningkatkan kemandirian daerah.BSSN selaku koordinator keamanan siber nasional, akan berupaya untuk memberikan asistensi jika dibutuhkan. Lalu melalui monitoring keamanan siber nasional, BSSN juga secara aktif mengumpulkan informasi insiden siber dan kerentanan sistem dari berbagai sumber sebagai bahan perbaikan sistem pada *stakeholder* termasuk pemerintah daerah.

B. Simulasi Penerapan Elastic Stack

Dalam penerapan pada tulisan ini, Penulis menggambarkan pemanfaatan Elastic Stack untuk mengumpulkan log pada sistem operasi Linux Ubuntu 16.04 64-bit yang menjalankan *service* aplikasi web dan *database*, sehingga log yang

 p-ISSN : 2502-5724; e-ISSN : 2541-5735

dihasilkan dari OS dan aplikasi tersebut dapat dianalisis untuk kepentingan monitoring dan respon insiden. Aplikasi web dan *database* milik pemerintah merupakan hal yang paling sering menjadi sasaran serangan siber karena sarat akan kerentanan.

Simulasi ini memanfaatkan dua buah sistem operasi Ubuntu Server 16.04 64 bit. Masing-masing OS menggunakan sumber daya komputasi 4 CPU 2,20 GHz dan RAM 4 GB. Ubuntu pertama (Ubuntu sensor) akan berlaku sebagai web server yang menjalankan *service* aplikasi web Apache dan *database* MySQL. Lalu pada server tersebut dipasang Suricata, OSSEC, dan Beats untuk keperluan monitoring dan pengiriman data. Lalu Ubuntu kedua (Ubuntu ELK) adalah tempat pengumpulan log yang telah dipasangi Elasticsearch, Logstash, dan Kibana sebagai server monitoring dan *dashboard*.

Pada Ubuntu sensor telah dipasang Suricata versi 4.1.5 dengan *rules* milik Suricata per tanggal 7 Oktober 2019. *Rules* yang berlaku akan dicocokkan dengan paket-paket jaringan yang masuk ke *port* (*interface* jaringan) yang dimonitor Ubuntu sensor. Suricata menghasilkan log berupa *file* JSON yang akan dikirim ke Ubuntu ELK menggunakan Beats.

Pada Ubuntu sensor juga dipasang OSSEC sebagai HIDS. OSSEC yang digunakan adalah OSSEC versi 3.2.0 dengan mode *local/hybrid* (dengan mode ini, OSSEC dapat berlaku sebagai OSSEC Server maupun OSSEC *agent*). OSSEC juga menghasilkan log berupa JSON. *File* inilah yang akan dikirim ke Ubuntu ELK menggunakan Beats.

Untuk mengirimkan log Suricata dan OSSEC, dipasang Beats untuk mengirim *file* yaitu Filebeat versi 6.6.1. Filebeat dikonfigurasi untuk mengirim kedua *file* JSON dari Suricata dan OSSEC kepada Logstash yang dipasang di Ubuntu ELK.

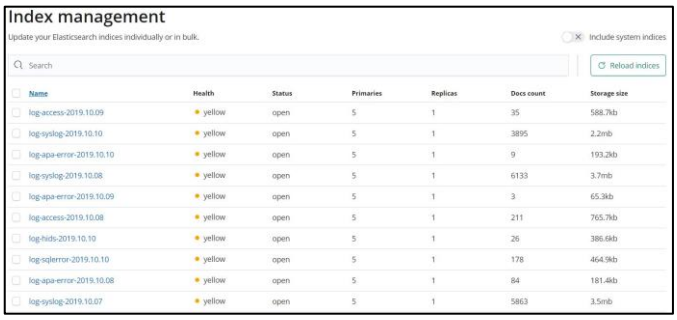
Selain kedua log dari Suricata dan OSSEC, Tabel 1 menunjukkan log-log aplikasi dan OS pada web server yang dikirim ke Ubuntu ELK untuk dimonitor dan keperluan respon insiden.

Logstash dikonfigurasi untuk menerima input dari Filebeat dan melakukan *parsing* data sesuai dengan tipe log. Data yang di-*parsing* oleh Logstash disimpan ke Elasticsearch dengan nama indeks sesuai dengan variabel tipe lognya untuk memudahkan pembagian indeks seperti yang terlihat pada Gambar 5.

Selama menerima data, Elasticsearch diatur untuk membuat indeks setiap hari, sehingga setiap hari akan dibuat indeks baru. Setiap data di dalam indeks akan dikelompokkan dalam masing-masing *field*. Pembagian *field* dibuat untuk memudahkan pembuatan visualisasi data. Sebagai contoh visualisasi *map* yang dibuat dengan menghitung jumlah *field* "*destination.geo.ip*" yang muncul dari indeks Suricata "log-nids", sehingga menghasilkan pemetaan dan jumlah kemunculan dari alamat IP apa saja yang diakses oleh server dan kode negaranya seperti yang terlihat pada Gambar 6.

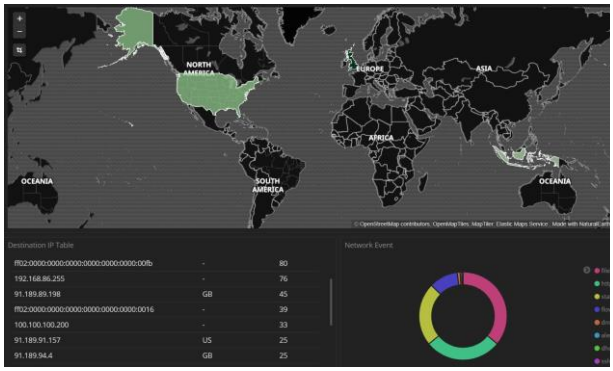
Tabel 1. *Log* yang dikirim ke ELK

Aplikasi/OS	Log	Keterangan
Apache	access.log	*Record* setiap halaman yang dibuka oleh *web server*
	error.log	*Error* HTTP Server
MySQL	mysql.log	*Command* SQL
	error.log	*Error* MySQL
Ubuntu OS	auth.log	*User login and sudo command*
	syslog	*System Logs*
	kern.log	Linux kernel

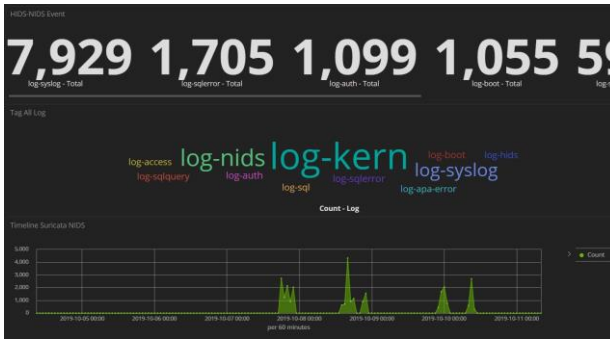


Gambar 5. Daftar indeks pada Elasticsearch

Kibana berfungsi sebagai *dashboard* monitoring yang di dalamnya terdapat sekumpulan visualisasi data. *Dashboard* menampilkan data dalam berbagai macam bagan untuk memudahkan *user* memonitor *event-event* yang ada pada *traffic* jaringan dan *host*. Pada Gambar 7 dapat terlihat visualisasi dari total *event* dari semua log yang dikumpulkan. Selanjutnya terdapat visualisasi *timeline* jumlah *event* Suricata untuk melihat pada waktu-waktu apa saja *event* muncul secara signifikan.



Gambar 6. Visualisasi map destination IP



Gambar 7. Visualisasi total event log

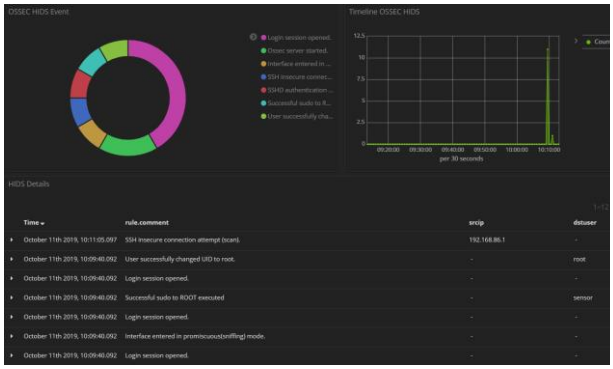
Gambar 8. Visualisasi Alert Suricata, Network Event, dan Detail Event

Gambar 8 menunjukkan bagan *pie chart* yang berisi jenis *event* yang muncul dari Suricata dan *event alert* yang menampilkan adanya anomali pada jaringan yang dimonitor beserta detailnya. *Use case* pada bagan di atas menunjukkan adanya anomali suatu IP yang melakukan koneksi ke banyak *port* pada server, sehingga diindikasikan bahwa terdapat percobaan *scanning* jaringan ke server.

Gambar 9 menunjukkan bagan *pie chart* dari *event* yang terjadi pada *host* serta *timeline* log OSSEC dan detailnya. *Use case* dari visualisasi tersebut adalah laporan *login session* ke sistem dan adanya percobaan *insecure login* SSH ke server.

Gambar 10 menunjukkan log *request* dan *response* web server Apache. *Use case* pada visualisasi tersebut terdapat *request* dari *client* menuju ke halaman yang tidak tersedia dan mendapat respon *error* 404, sehingga diindikasikan bahwa *client* tersebut mencoba melakukan *information gathering* terhadap server dan mencari halaman yang dapat dieksploitasi.

p-ISSN : 2502-5724; e-ISSN : 2541-5735



Gambar 9. Visualisasi Event OSSEC, Timeline Event OSSEC, dan Detail Event OSSEC

Gambar 10, Visualisasi log Apache

Gambar 11. Visualisasi log MySQL

Gambar 12. Visualisasi log sistem

Gambar 11 menunjukkan log dari aplikasi MySQL yang berisi pesan *error* dan *command* SQL yang di-*request* oleh *client*. *Use case* pada visualisasi tersebut adalah terdapat *client* yang melakukan *request bypass login.*

Selain log dari aplikasi, NIDS dan HIDS, log dari sistem juga dapat memberikan informasi penting guna monitoring dan respon insiden seperti pada Gambar 12. Log sistem seperti “auth.log” memberikan informasi tentang *user login* dan menginfokan jika terdapat *login* yang berhasil dan gagal. Contoh *use case* adalah jika terdapat *login* gagal dalam jumlah yang banyak, dapat diindikasikan bahwa terdapat *user* yang mencoba melakukan serangan *brute force login* ke sistem.

Sebagai media pengumpulan log dan penyajian data, Elastic Stack sudah cukup mumpuni dan mudah untuk diterapkan. Kekurangan dari Elastic Stack adalah dibutuhkan usaha tambahan untuk melakukan korelasi secara manual dari semua log yang ada. Korelasi dilakukan untuk mempermudah pengambilan kesimpulan terhadap suatu insiden. Kekurangan lain adalah *user* harus melakukan konfigurasi manual untuk melakukan *parsing* log dengan Logstash. Format log yang beragam membutuhkan filter yang berbeda untuk dapat disajikan oleh Kibana.

Dalam melakukan monitoring dan respon insiden, tentunya selain membutuhkan teknologi, diperlukan juga personil yang mengerti tentang sistem dan keamanan siber. Pengalaman personil sangat dibutuhkan untuk dapat memahami setiap *event* pada log, karena setiap *event* harus diverifikasi untuk meminimalisir *false positive*.

4. PENUTUP

A. Kesimpulan

Berdasarkan hal-hal yang Penulis uraikan pada bab-bab sebelumnya, dapat disimpulkan bahwa Konsep pola koordinasi pemantauan dan respon insiden siber di setiap instansi pemerintah Indonesia perlu diatur oleh BSSN, di mana setiap instansi pemerintah diharapkan membangun SOC (minimal penerapan sistem pemantauan *traffic* dan *host*) masing-masing yang dikoordinasikan oleh BSSN sehingga terbentuk kemandirian dalam keamanan siber.

Kemudian, penerapan teknologi pemantauan *traffic* jaringan, *host*, serta pengumpulan log memanfaatkan Suricata, OSSEC, dan Elastic Stack berjalan lancar pada skala laboratorium. Suricata dan OSSEC berhasil membangkitkan log yang berisi *alert* dan *event*. Elastic Stack juga dapat mengolah dan memvisualisasikan log yang berasal dari Suricata, OSSEC, Apache, MySQL dan OS Ubuntu dengan baik sehingga memudahkan *user* dalam menganalisis data guna melakukan monitoring dan respon insiden.

B. Saran

Beberapa saran yang dapat menjadi masukan antara lain:

1. Hendaknya rekomendasi pola koordinasi yang Penulis sampaikan dapat menjadi bahan pertimbangan dalam menyusun kebijakan guna membentuk kemandirian dalam hal keamanan siber dan mewujudkan ketahanan siber nasional.
2. Perlunya dilakukan eksplorasi lebih jauh tentang fitur-fitur Suricata, OSSEC, dan Elastic Stack untuk memaksimalkan analisis dan performa dalam melakukan monitoring. Perlu dipelajari fitur tambahan yang akan sangat berguna seperti *alerting* dan korelasi *event*.

5. REFERENSI

APJII, A. P. J. I. I. (2018). *Penetrasi & perilaku pengguna internet indonesia*.

Babu, J. B., Prasad, S., & Prasad, G. S. (2019). *Detecting and Analyzing the Malicious Linux Events using Filebeat and ELK Stack*. https://www.ijeat.org/wp-content/uploads/papers/v8i4/D7003048419.pdf

Bara Hitapuru. (2018). *Analisis Kemampuan Security Operations Center (SOC) Sebagai Sistem Pertahanan Siber Dalam Mengatasi Ancaman Serangan Siber Di Indonesia*. Universitas Indonesia.

Chen, Y., Chong, P. P., & Zhang, B. (2004). *Cyber security management and e-government*. *1*(3), 316–327.

Deputi Bidang Proteksi BSSN. (2018). *Transformasi Lembaga Sandi Negara Menjadi Badan Siber dan Sandi Negara*. Focus Group Discussion Proteksi, Penanggulangan, dan Pemulihan Insiden Siber Sektor Pemerintah. https://govcsirt.bssn.go.id/download/Transformasi-Lemsaneg-menjadi-BSSN-signed.pdf

Elahi, U. (t.t.). *Elastic Stack—A Brief Introduction*. Diambil 11 Oktober 2019, dari https://hackernoon.com/elastic-

stack-a-brief-introduction-794bc7ff7d4f

Elasticsearch B.V. (2019a). *An Introduction to the ELK Stack for Logs and Metrics*. https://www.elastic.co/webinars/introduction-elk-stack

Elasticsearch B.V. (2019b). *Getting started with the Elastic Stack*. https://www.elastic.co/guide/en/elastic-stack-get-started/current/get-started-elastic-stack.html

Elasticsearch B.V. (2019c). *What is the ELK Stack? Why, it's the Elastic Stack.* https://www.elastic.co/what-is/elk-stack

Grigorof, A. (2019). *Open Source / Free Security Controls—Version 1.4*. http://www.eventid.net/docs/open_source_security_controls.asp

Harikanth, M., & Rajarajeswari, P. (2019). *Malicious Event Detection Using ELK Stack Through Cyber Threat Intelligence*.

Hootsuite, & We are social. (2019). *Digital 2019*.

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing*, *1*, 47–63. https://doi.org/10.1016/j.promfg.2015.09.060

Id-SIRTII. (2018). *Laporan Tahunan Id-SIRTII Tahun 2018*.

Peraturan Pemerintah Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, (2012).

Undang—Undang nomor 23 tahun 2014 tentang Pemerintah Daerah, (2012).

Kominfo. (2017). *Tren Serangan Siber Nasional 2016 dan Prediksi 2017*.

Kumar, V., Srivastava, J., & Lazarevic, A. (2005). *Managing Cyber Threats Issues, Approaches and Challenges* (hlm. 4). Springer.

Open Information Security Foundation. (2019). *About Suricata*. https://suricata-ids.org/about/

OSSEC PROJECT TEAM. (2019). *Host Intrusion Detection for Everyone*. https://www.ossec.net/about/

Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara, Pub. L. No. 53 (2017).

Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara, (2018).

Praneeth, J. N., & Sreedevi, M. (2019). *Detecting and Analyzing the Malicious Windows Events using Winlogbeat and ELK Stack*. https://www.ijrte.org/wp-content/uploads/papers/v7i6s/F03400376S19.pdf

Raja, B., Ravindranath, K., & Jayanag, B. (2019). *Monitoring and Analysing Anomaly Activities in a Network using Packetbeat*. https://www.ijitee.org/wp-content/uploads/papers/v8i6s/F60190486S19.pdf

Sameer Dharur, & K Swaminathan. (2018). Efficient surveillance and monitoring using the ELK stack for IoT powered Smart Buildings. *Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)*, *CFP18J06-ART*. https://ieeexplore.ieee.org/document/8398888

Sudarmadi, D. A. (2018). *Strategi Badan Siber Dan Sandi Negara (Bssn) Dalam Menghadapi Ancaman Siber Di Indonesia*. Universitas Indonesia.