Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Integrasi SIEM & SOAR untuk Otomatisasi Pemblokiran IP Address pada Router MikroTik

Muhammad Mirza Albazi [1]*, Antoni Haikal [2]**
* Rekayasa Keamanan Siber, Politeknik Negeri Batam
** Politeknik Negeri Batam
muhammadmirzaalbazi@gmail.com [1], antoni@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

SIEM, SOAR, Threat Intelligence, MikroTik, IP Blocking.

ABSTRACT

The increasing sophistication of cyber threats and the enactment of Indonesia Law Number 27 of 2022 on Personal Data Protection require organizations to implement adequate security controls. PT XYZ has implemented a Security Information and Event Management (SIEM) system to monitor and analyze Indicators of Compromise (IoC) from internal servers. However, the response process and IP address blocking on MikroTik routers are still performed manually by the IT Division, leading to delayed responses and increased risk of data breaches. This study proposes the integration of SIEM and Security Orchestration, Automation, and Response (SOAR) to automate the threat response workflow, from IoC validation using threat intelligence to automatic IP address blocking execution on MikroTik routers via Application Programming Interface (API). The system was implemented in a UAT environment using Wazuh as SIEM, Shuffle as SOAR, MISP as threat intelligence, and a MikroTik RB951Ui-2nD router. System feasibility was evaluated using the User Acceptance Testing (UAT) method with a Likert scale-based questionnaire involving 14 respondents from all members of the IT Division of PT XYZ. The results show that all four evaluation variables system usability, ease of use, system reliability, and user satisfaction achieved scores in the "Very Good" category, with percentages of 88%, 87%, 90%, and 92% respectively. These findings indicate that the SIEM-SOAR integration system is well accepted and effective in automating IP address blocking as an initial step in mitigating cyber threats.

I. PENDAHULUAN

Keamanan informasi merupakan aspek krusial bagi organisasi di era digital, terlebih dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mewajibkan setiap organisasi menerapkan kontrol keamanan yang memadai. Ancaman siber yang semakin canggih mendorong kebutuhan akan solusi keamanan yang efektif dan terintegrasi, salah satunya melalui pemanfaatan *firewall* sebagai alat utama untuk mengontrol akses jaringan dan melindungi sistem dari ancaman eksternal [1]. *Router* MikroTik menjadi salah satu pilihan yang dikenal memiliki fitur kuat dan fleksibel dalam meningkatkan keamanan jaringan, termasuk kemampuan filter *rules* dan API untuk integrasi dengan sistem eksternal [2] [3] [4].

PT XYZ telah mengimplementasikan SIEM guna memantau dan menganalisis IoC dari server *endpoint* yang menjalankan layanan web profil dan web aplikasi PT XYZ. SIEM terbukti efektif dalam meningkatkan deteksi dan respons ancaman serta memastikan kepatuhan terhadap regulasi [5]. Namun, proses respons dan pemblokiran IP *address* pada *router* MikroTik masih dilakukan secara manual oleh Divisi IT, sehingga berpotensi menimbulkan keterlambatan respons dan meningkatkan risiko kebocoran data pribadi.

Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan integrasi SIEM dengan SOAR guna mengotomatisasi alur respons ancaman, mulai dari validasi IoC berbasis *threat intelligence* hingga eksekusi pemblokiran IP *address* secara otomatis pada MikroTik [6]. Integrasi

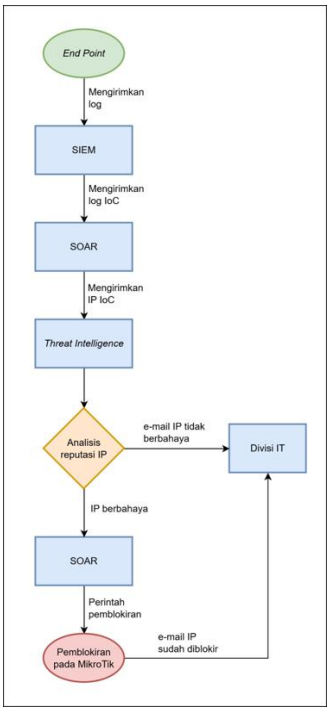
e-ISSN: 2548-6861

keempat komponen ini diharapkan membentuk sistem keamanan yang tangguh, mempercepat waktu respons, serta meminimalkan potensi *human error* dalam penanganan ancaman siber.

II. METODE

Penelitian ini menggunakan metodologi eksperimental yang bertujuan untuk mengukur efektivitas integrasi SIEM-SOAR dalam mengotomatisasi pemblokiran IP *address*. Metode ini dipilih karena penelitian ini berfokus pada pengembangan solusi respons ancaman secara langsung di lingkungan UAT, kemudian mengukur hasilnya secara kualitatif. Pendekatan ini memungkinkan peneliti untuk mengevaluasi persepsi dari Divisi IT PT XYZ terhadap sistem yang dibagun.

Penelitian ini berfokus pada perancangan dan pengintegrasian SIEM dan SOAR di PT XYZ dalam menganalisis IoC yang terdeteksi secara *real-time* melalui platform SIEM, kemudian memicu proses respons otomatis oleh SOAR berdasarkan analisis IP *address* dari *threat intelligence*. Hasil analisis tersebut akan diteruskan ke *router* MikroTik oleh SOAR melalui API untuk mengeksekusi *rule* pemblokiran IP *address* secara otomatis seperti flowchart pada Gambar 1.



Gambar 1 - Perencanaan flowchart

A. Studi Literatur

1). Keamanan Siber

Keamanan siber merupakan upaya melindungi sistem, jaringan, dan data dari serangan atau akses yang tidak sah, dengan prinsip utama *confidentiality*, *integrity*, dan *availability* [7]. Dalam konteks operasional, respons ancaman menjadi bagian penting untuk mendeteksi dan menanggulangi ancaman secara cepat agar dampak serangan dapat diminimalkan. Proses ini umumnya dilakukan oleh Tim Security Operation Center (SOC) melalui analisis log yang terdeteksi.

2). SIEM

SIEM adalah sistem yang berfungsi untuk mengumpulkan, mengkorelasi, dan menganalisis data log dari berbagai sumber untuk mendeteksi dan menanggapi ancaman secara *real-time*. Teknologi ini dapat meningkatkan deteksi dan respons ancaman, memastikan kepatuhan terhadap regulasi, dan meningkatkan efisiensi operasional [5]. Contoh implementasi SIEM seperti Wazuh atau Splunk mampu memberikan visibilitas menyeluruh terhadap status keamanan sistem.

3.) SOAR

SOAR merupakan keharusan strategis untuk membangun arsitektur keamanan yang tangguh, proaktif, dan cerdas. Platform ini melengkapi SIEM dengan mengotomatisasikan proses respons ancaman. Integrasi SOAR membantu Tim SOC mengurangi *Mean Time To Respond* (MTTR) [8].

4.) Threat Intelligence

Threat intelligence mencakup kegiatan pengumpulan, pemrosesan, dan analisis data untuk memahami motif, perilaku, serta target dari pelaku ancaman, sehingga dapat memberikan wawasan yang dapat ditindaklanjuti guna mencegah dan menanggulangi kejahatan siber [9]. Dengan menambahkan *threat intelligence* pada sistem ini, maka dapat memvalidasi IoC yang terdeteksi.

5.) MikroTik

MikroTik merupakan sistem operasi *router* yang dirilis dengan nama RouterOS yang dapat diinstal pada komputer biasa. MikroTik memiliki fitur yang sangat lengkap, diantaranya *firewall*, *Network Address Translation* (NAT), *routing*, *hotspot*, *point to point tunneling protocol*, *Domain Name System* (DNS) server, *Dynamic Host Configuration Protocol* (DHCP) server, dan manajemen *bandwidth* [10]. Selain itu MikroTik juga menyediakan API untuk diintegrasikan ke platform lain [4].

6.) UAT

UAT adalah metode pengujian yang dilakukan oleh *end user* untuk memastikan sistem yang dikembangkan telah memenuhi kebutuhan fungsional yang telah ditetapkan sebelum sistem diterapkan secara resmi [11]. UAT berfokus pada penilaian kelayakan fungsional sistem dari sudut pandang pengguna, bukan dari sudut pandang pengembang. Dalam penelitian eksperimental ini, UAT digunakan sebagai instrumen evaluasi kualitatif untuk mengukur tingkat penerimaan pengguna terhadap sistem yang dikembangkan.

Dalam pelaksanaannya, instrumen kuesioner UAT disusun berdasarkan variabel-variabel tertentu yang merepresentasikan aspek-aspek penilaian sistem secara menyeluruh. Mengacu pada praktik yang digunakan oleh [11], penggunaan 25 daftar kuesioner yang terdistribusi ke dalam beberapa variabel pengukuran merupakan jumlah yang representatif digunakan dalam penelitian UAT pada sistem informasi.

7.) Skala Likert

Skala Likert merupakan alat ukur psikometrik yang paling umum digunakan dalam penelitian untuk mengukur persepsi atau pendapat responden terhadap suatu objek. [12] menjelaskan bahwa banyak peneliti keliru menyebut semua skala bertingkat sebagai skala Likert, padahal skala Likert memiliki karakteristik spesifik yaitu menggunakan pernyataan dengan pilihan jawaban yang bersifat ordinal dan berjenjang, di mana setiap jenjang merepresentasikan tingkat persetujuan atau ketidak setujuan responden terhadap pernyataan yang diajukan. [12] juga menegaskan bahwa instrumen pengukuran berbasis skala Likert harus melibatkan sejumlah item pertanyaan atau pernyataan, bukan item tunggal, agar konstruk variabel yang diukur dapat direpresentasikan secara valid dan reliabel.

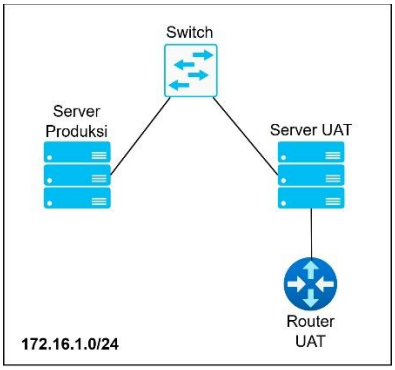
B. Langkah Penelitian

Metodologi eksperimental dalam penelitian ini terdiri dari tiga tahapan, yaitu :

1.) Perencanaan

Pada tahap pertama, peneliti memfokuskan pada persiapan dan analisis awal, meliputi :

- Studi Literatur : Peneliti melakukan kajian literatur terkait pengintegrasian SIEM, SOAR, *threat intelligence*, dan *router* MikroTik.
- Analisis Infrastruktur Sistem : Peneliti mempelajari dan menganalisis sistem dan topologi yang diterapkan di PT XYZ.
- Perancangan Topologi : Peneliti merancang topologi seperti pada Gambar 2.



Gambar 2 - Rancangan Topologi

- Perancangan Instrumen UAT : Peneliti merancang instrumen kuesioner UAT berbasis skala Likert 5 poin yang mencakup empat variabel pengukuran, yaitu : kegunaan sistem, kemudahan penggunaan, keandalan sistem, dan kepuasan pengguna.

2.) Implementasi dan Uji Coba

Pada tahap ini, peneliti melakukan proses integrasi antara SIEM, SOAR, *threat intelligence*, dan *router* MikroTik, yang mencakup :

- Instalasi dan Integrasi : Melakukan instalasi SOAR (Shuffle) dan *threat intelligence* (MISP) serta konfigurasi integrasi antara SIEM, SOAR, *threat intelligence*, dan *router* MikroTik agar proses respons dapat berjalan secara otomatis.
- Pengujian Awal : Peneliti melakukan pengujian internal terhadap sistem yang sudah diintegrasikan, pengujian ini bertujuan untuk memastikan bahwa sistem sudah berjalan dengan baik.
- Pengukuran Efektivitas : Peneliti mengukur MTTR dari 10 simulasi serangan yang diuji coba ke salah 1 server internal dan membandingkan antara respons manual dan otomatis mulai dari IoC terdeteksi sampai pemblokiran IP *address* di MikroTik.
- Dokumentasi Teknis : Peneliti menyusun dokumentasi teknis terkait proses instalasi, konfigurasi, dan hasil pengujian untuk dijadikan panduan bagi Tim SOC PT XYZ.

3.) Evaluasi

Tahap evaluasi menggunakan metode UAT untuk menilai persepsi Divisi IT terhadap sistem yang dibangun. Evaluasi dilakukan secara kualitatif menggunakan instrumen kuesioner berbasis skala Likert untuk mengukur tingkat penerimaan pengguna terhadap sistem setelah demonstrasi langsung [11].

- Responden : Responden dalam pengujian ini adalah seluruh anggota Divisi IT PT XYZ yang terlibat langsung dalam penggunaan sistem ini yang berjumlah 14 orang.
- Instrumen Kuesioner : Instrumen kuesioner UAT ini dikembangkan berdasarkan dari variabel evaluasi penerimaan pengguna yang digunakan oleh [11], kemudian disesuaikan dengan konteks sistem integrasi SIEM dan SOAR. Kuesioner ini terdiri dari 25 pertanyaan, sebagaimana pada Tabel 1.

No.	Variabel	Pertanyaan	Kode
1	Kegunaan Sistem	Apakah sistem otomatisasi ini membantu mempercepat proses pemblokiran IP *address* berbahaya dibandingkan proses manual sebelumnya?	A1
2		Apakah sistem ini meningkatkan efisiensi	A2

e-ISSN: 2548-6861

		kerja Tim SOC dalam menangani IoC?	
3		Apakah sistem ini bermanfaat dalam mengurangi beban kerja manual Tim SOC?	A3
4		Apakah sistem ini mendukung pemenuhan kebutuhan keamanan jaringan PT XYZ secara keseluruhan?	A4
5		Apakah dengan adanya sistem ini, Tim SOC dapat lebih fokus pada analisis ancaman dibandingkan eksekusi manual pemblokiran IP *address*?	A5
6		Apakah sistem ini membantu mengurangi risiko keterlambatan dalam penanganan ancaman siber?	A6
7		Apakah sistem ini berkontribusi dalam menurunkan potensi terjadinya *human error* pada proses pemblokiran IP *address*?	A7
8	Kemudahan Penggunaan	Apakah dashboard SOAR mudah dipahami dan digunakan oleh anggota Divisi IT?	B1
9		Apakah alur kerja otomatisasi pada SOAR mudah dipahami oleh Divisi IT?	B2
10		Apakah proses monitoring log ancaman pada SIEM dapat dilakukan dengan mudah?	B3
11		Apakah sistem ini dapat dioperasikan tanpa memerlukan pelatihan teknis yang terlalu ekstensif?	B4
12		Apakah *alert* yang dihasilkan sistem mudah diinterpretasikan oleh Tim SOC?	B5
13		Apakah sistem secara keseluruhan sudah cukup intuitif dan tidak membingungkan pengguna?	B6
14	Keandalan Sistem	Apakah selama periode pengujian demo, sistem berjalan stabil tanpa gangguan berarti?	C1
15		Apakah pemblokiran IP *address* dilakukan secara akurat sesuai dengan hasil validasi *threat intelligence*?	C2
16		Apakah sistem tidak mengalami kegagalan selama proses otomatisasi berlangsung?	C3
17		Apakah *alert* dari sistem berjalan sesuai dengan yang diharapkan?	C4
18		Apakah sistem mampu mendeteksi dan merespons ancaman secara konsisten pada setiap skenario pengujian?	C5
19		Apakah integrasi antara SIEM, SOAR, threat intelligence, dan router MikroTik berjalan tanpa hambatan teknis yang signifikan?	C6
20	Kepuasan Pengguna	Apakah Anda merasa puas dengan kinerja sistem otomatisasi ini secara keseluruhan?	D1
21		Apakah sistem ini memenuhi ekspektasi Anda sebagai pengguna dari Divisi IT PT XYZ?	D2
22		Apakah Anda merekomendasikan sistem ini untuk diterapkan di lingkungan produksi PT XYZ?	D3
23		Apakah sistem ini meningkatkan kepercayaan Anda	D4

		terhadap keamanan jaringan PT XYZ?	
24		Apakah Anda merasa sistem ini layak dijadikan bagian tetap dari infrastruktur keamanan siber PT XYZ?	D5
25		Apakah secara keseluruhan sistem integrasi SIEM-SOAR ini memberikan nilai tambah yang nyata bagi operasional keamanan PT XYZ?	D6

Tabel 1 - Daftar Kuesioner

- Pengumpulan Data : Pengumpulan data dilakukan melalui demonstrasi sistem kepada seluruh anggota Divisi IT PT XYZ, dilanjutkan dengan pengisian kuesioner UAT. Demonstrasi mencakup penjelasan alur kerja sistem dari deteksi IoC oleh SIEM hingga eksekusi pemblokiran IP *address* pada *router* MikroTik.
- Analisis Data : Data kuesioner dianalisis menggunakan langkah-langkah sebagai berikut :

a. Menghitung nilai total untuk setiap pertanyaan dari variabel menggunakan rumus : Nilai Total = Skor x Frekuensi.
b. Menghitung nilai persentase dari 25 kuesioner menggunakan rumus :
Nilai Rata-rata = Nilai total / Total Responden
Persentase = Nilai Rata-Rata / Bobot Maksimum x 100%.
c. Menginterpretasikan nilai dari setiap variabel keseluruhan berdasarkan rentang skala Likert : 0% – 20% (Sangat Kurang Baik), 21% – 40% (Kurang Baik), 41% – 60% (Cukup Baik), 61% - 80% (Baik), dan 81% - 100% (Sangat Baik).

C. Perancangan Sistem

1.) Arsitektur Sistem

Arsitektur sistem yang dirancang terdiri dari empat komponen utama yang saling terintegrasi, yaitu SIEM (Wazuh), SOAR (Shuffle), *threat intelligence* (MISP), dan *router* MikroTik. Alur kerja sistem secara umum adalah sebagai berikut :

1. Server endpoint mengirimkan log secara *real-time* ke Wazuh.
2. Wazuh menganalisis log yang masuk dan mengkategorikan berdasarkan *rule* IoC.
3. IoC dari Wazuh ditruskan ke Shuffle yang secara otomatis akan memicu workflow yang sudah dirancang.
4. Shuffle melakukan validasi IP *address* menggunakan MISP untuk memverifikasi reputasi IP *address* tersebut.
5. Apabila reputasi IP *address* tersebut tidak tergolong berbahaya, maka akan dikirimkan e-mail agar dianalisis lebih lanjut.
6. Apabila reputasi IP *address* tersebut termasuk berbahaya, maka Shuffle akan mengeksekusi perintah pemblokiran IP *address* tersebut ke *router* MikroTik dan akan mengirimkan e-mail pemberitahuan jikalau IP tersebut sudah diblokir.

2.) Perancangan Workflow SOAR

Workflow Shuffle dirancang untuk mengotomatisasi alur respons ancaman secara menyeluruh. *Workflow* terdiri dari *node-node* yang saling terhubung, meliputi : penerimaan *webhook alert* dari Wazuh, ekstraksi IP *address* dari *alert*, pengecekan reputasi IP *address* ke MISP, eksekusi perintah pemblokiran ke *router* MikroTik, dan pengiriman e-mail kepada Divisi IT.

3.) Spesifikasi Perangkat dan Platform

- Server UAT : Intel Core i5 Quad Core, HDD 1 TB, RAM 16 GB, Ubuntu Server 22.04.
- SIEM : Wazuh.
- SOAR : Shuffle yang dijalankan menggunakan docker di server UAT.
- Threat Intelligence : MISP yang dijalankan menggunakan docker di server UAT.
- Router : MikroTik RB951Ui-2nD.

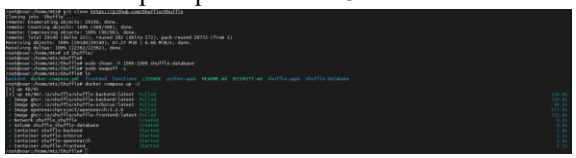
III. HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil dan pembahasan penelitian yang berfokus pada implementasi dan pengujian kelayakan sistem dengan metode UAT.

A. Implementasi Sistem

1.) Instalasi Shuffle

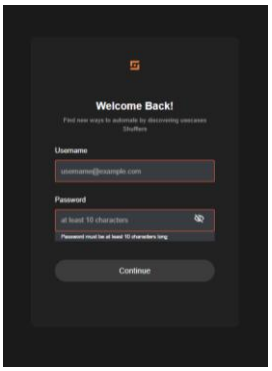
a. Sebelum melakukan instalasi shuffle, pastikan server sudah terinstal docker dan git.
b. Instalasi shuffle dengan mengetikan beberapa command seperti pada Gambar 3.



Gambar 3 - Instalasi Shuffle

c. Akses shuffle dan ketika pertama kali diakses harus membuat user baru seperti pada Gambar 4.

e-ISSN: 2548-6861



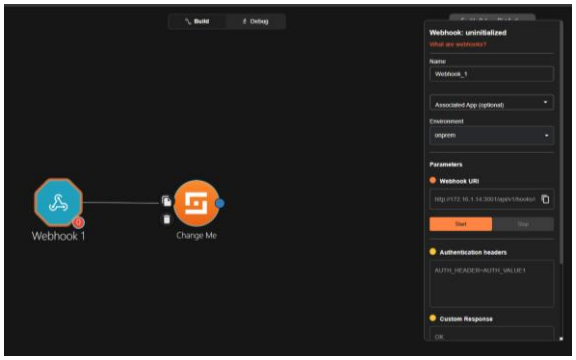
Gambar 4 - Pembuatan *User* Shuffle

d. Buat workflow baru seperti pada Gambar 5.

Gambar 5 - Pembuatan *Workflow*

2.) Integrasi Shuffle dengan Wazuh

a. Masukan *node webhook* dan salin *Webhook* URI-nya seperti pada Gambar 6 untuk mengintegrasikan dengan wazuh.



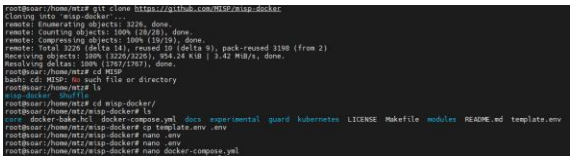
Gambar 6 - Integrasi Wazuh dan Shuffle

b. Edit file /var/ossec/etc/ossec.conf di server wazuh dan sesuaikan dengan IoC yang ingin dikirimkan ke shuffle seperti pada Gambar 7.

Gambar 7 - Konfigurasi Wazuh

3.) Instalasi MISP

a. Pada proses instalasi MISP di Gambar 8, ada beberapa perubahan di file .env untuk memasukan IP *address* server, terlihat pada Gambar 9 dan di file docker-compose.yml untuk mematikan port 80 terlihat pada Gambar 10.

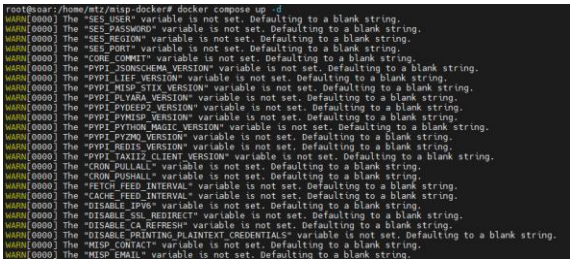


Gambar 8 - Instalasi MISP

Gambar 9 - Konfigurasi IP MISP

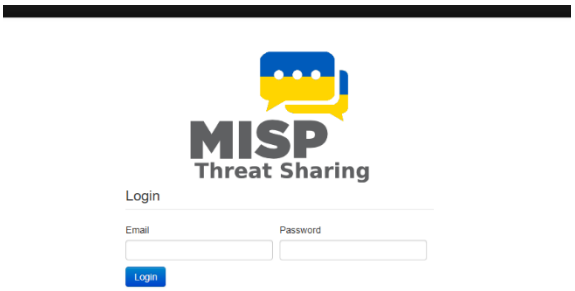
Gambar 10 - Konfigurasi *Port* MISP

b. Jalankan MISP dan tunggu prosesnya seperti pada Gambar 11.



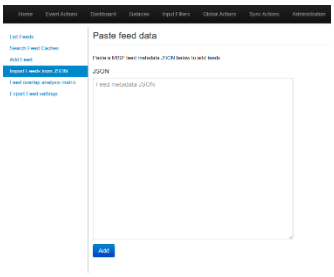
Gambar 11 - Menjalankan MISP

c. Akses MISP dan buat *user*-nya seperti pada Gambar 12.



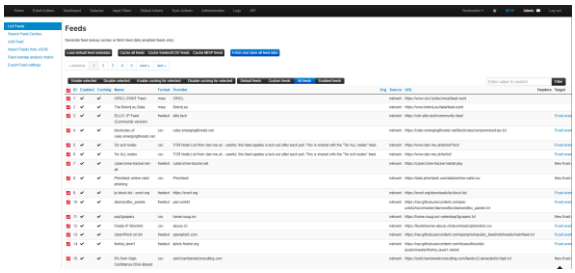
Gambar 12 - Pembuatan *User* MISP

d. *Import feeds* seperti pada Gambar 13 untuk memasukan sumber data sesuai list https://github.com/MISP/MISP/blob/2.4/app/files/feed-metadata/defaults.json.



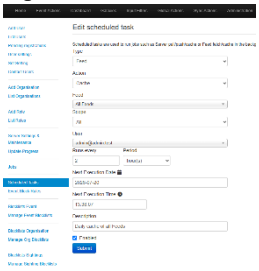
Gambar 13 - *Import Feeds*

e. Aktifkan *feeds* dengan cara ceklist semua *feeds* lalu *enable* dan *fetch and store all feed* seperti pada Gambar 14.



Gambar 14 - Aktivasi *Feeds*

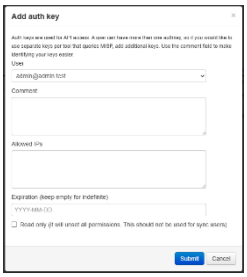
f. Aktifkan fitur *scheduled task* agar data *feeds*-nya terupdate seperti pada Gambar 15.



Gambar 15 - *Scheduled Task*

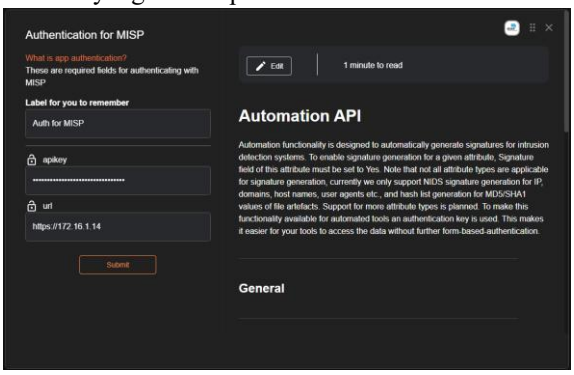
4.) Integrasi Shuffle dangan MISP

a. Buat *auth key* untuk integrasi ke shuffle seperti pada Gambar 16.

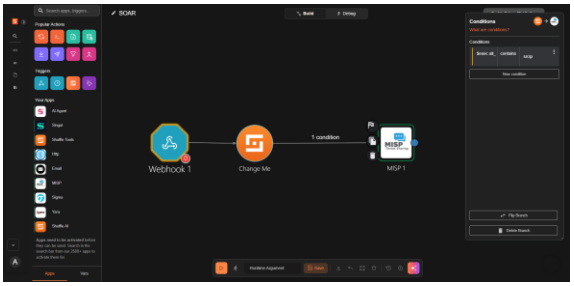


Gambar 16 - Pembuatan *Auth Key*

b. Tambahkan *node* MISP beserta *auth key*-nya seperti pada Gambar 17 dan juga kondisi seperti pada Gambar 18 untuk memfilter IoC yang hanya berisi *source* IP *address* yang akan diproses.



Gambar 17 - Integrasi MISP dan Shuffle



Gambar 18 - Filter IoC

5.) Konfigurasi Router MikroTik

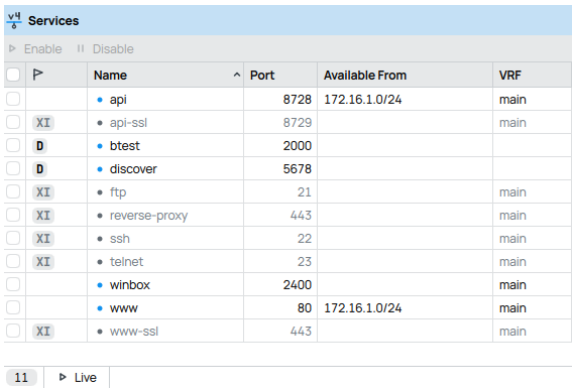
a. Buat filter *rules* untuk pemblokiran list IP *address* seperti pada Gambar 19.

```
[redacted] > ip firewall/filter/add action=drop chain=forward src-address
s-list=MALICIOUS
[redacted] >
```

Gambar 19 - Pembuatan Filter *Rules*

b. Aktifkan *services* api dan www untuk integrasi ke shuffle seperti pada Gambar 20.

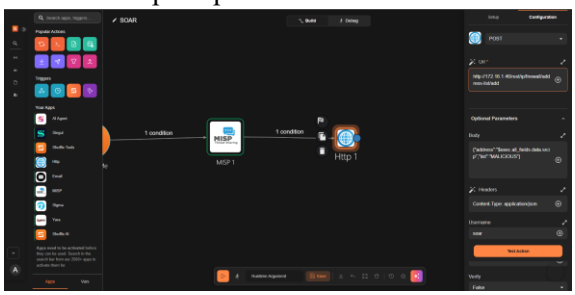
e-ISSN: 2548-6861



Gambar 20 - Konfigurasi *Services*

6.) Integrasi Shuffle dengan *Router* MikroTik

a. Tambahkan *node* Http dengan konfigurasi POST beserta parameter *Url*, *Body*, *Username*, dan *Password* seperti pada Gambar 21.



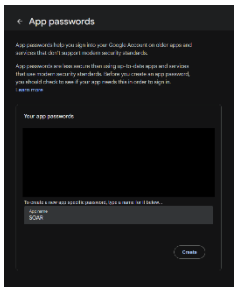
Gambar 21 - Integrasi MikroTik dan Shuffle

b. Tambahkan kondisi untuk memfilter hanya IP *address* yang terindikasi berbahaya saja yang akan diblokir di *router*.

Gambar 22 - Kondisi Pemblokiran IP

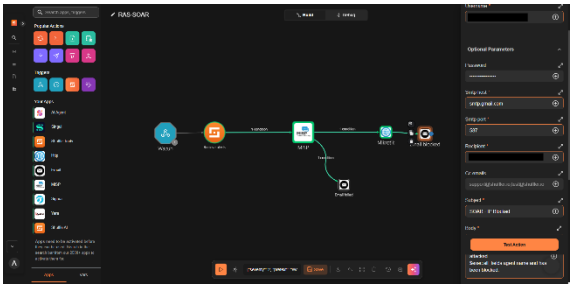
7.) Integrasi E-mail

a. Buat *app password* gmail untuk diintegrasikan ke shuffle seperti pada Gambar 23.



Gambar 23 - Pembuatan *App Password*

b. Tambahkan *node* Email setelah *node* MikroTik sebagai memberitahuan IP *address* berbahaya sudah diblokir seperti pada Gambar 24 dan setelah *node* MISP seperti pada Gambar 25 untuk mengirimkan e-mail jika IP *address* tidak terindikasi berbahaya, agar bisa dilakukan pengecekan lebih lanjut oleh tim SOC.



Gambar 24 - Konfigurasi E-mail jika IP Sudah Diblokir

Gambar 25 - Konfigurasi E-mail jika IP Tidak Berbahaya

B. Pengujian Efektifitas Sistem

1.) Pengukuran MTTR

Pengujian kuantitatif dilakukan terhadap 10 simulasi serangan dan kemudian hasilnya dibandingkan antara pengukuran MTTR otomatis dan MTTR manual dan hasilnya dirangkum pada Tabel 2.

Simulasi	MTTR Otomatis (detik)	MTTR Manual (detik)	Selisih (detik)
10 serangan	30,9	101,7	70,8

Tabel 2 - Perbedaan MTTR Otomatis dan Manual

C. Pengujian Kelayakan Sistem

1.) Perhitungan UAT

Untuk menguji kelayakan sistem yang sudah dibangun, dilakukan pengujian lanjutan menggunakan metode UAT dengan melibatkan 14 rsponden dari Divisi IT pada PT XYZ. Masing-masing responden diminta untuk mengisi kuesioner dengan bobot nilai 1 – 5, dengan rincian pada Tabel 3.

Bobot	Keterangan
1	Tidak Setuju
2	Kurang Setuju
3	Cukup Setuju
4	Setuju
5	Sangat Setuju

Tabel 3 - Bobot Penilaian Skala *Likert*

Dari data kuesioner yang sudah didapat, kemudian dianalisis dengan menghitung nilai total yang diperoleh dari setiap jawaban responden dengan mengelompokan tiap variabel kuesioner seperti pada Tabel 4 – 7.

Kode	5xF	4xF	3xF	2xF	1xF	Jumlah
A1	40	24	0	0	0	64
A2	40	24	0	0	0	64
A3	35	28	0	0	0	63
A4	45	20	0	0	0	65
A5	30	32	0	0	0	62
A6	45	20	0	0	0	65
A7	30	24	0	0	0	54

Tabel 4 - Variabel Kegunaan Sistem

Kode	5xF	4xF	3xF	2xF	1xF	Jumlah
B1	30	32	0	0	0	62
B2	30	32	0	0	0	62
B3	40	24	0	0	0	64
B4	15	28	12	0	0	55
B5	40	20	3	0	0	63
B6	30	28	3	0	0	61

Tabel 5 - Variabel Kemudahan Penggunaan

Kode	5xF	4xF	3xF	2xF	1xF	Jumlah
C1	40	20	3	0	0	63
C2	30	32	0	0	0	62
C3	40	20	3	0	0	63
C4	35	28	0	0	0	63
C5	40	20	3	0	0	63
C6	40	24	0	0	0	64

Tabel 6 - Variabel Keandalan Sistem

Kode	5xF	4xF	3xF	2xF	1xF	Jumlah
D1	50	16	0	0	0	66
D2	40	24	0	0	0	64
D3	40	24	0	0	0	64
D4	40	24	0	0	0	64
D5	50	16	0	0	0	66
D6	35	28	0	0	0	63

Tabel 7 - Variabel Kepuasan Pengguna

2.) Interpretasi Skor

Setelah dilakukan perhitungan nilai total dari hasil UAT, langkah selanjutnya adalah menginterpretasikan hasil tersebut agar dapat memberikan gambaran tentang tingkat penerimaan dan kelayakan sistem. Kriteria interpretasi tersaji pada Tabel 8.

Peresentase	Keterangan
0% - 20%	Sangat Kurang Baik
21% - 40%	Kurang Baik
41% - 60%	Cukup Baik
61% - 80%	Baik
81% - 100%	Sangat Baik

Tabel 8 - Interpretasi Skor

Berikut interpretasi dari masing-masing variabel yang sudah dihitung seperti pada Tabel 9 – 12.

Kode	Nilai Rata-rata	Persentase
A1	4,6	92%
A2	4,6	92%
A3	4,5	90%
A4	4,6	92%
A5	4,4	88%
A6	4,6	92%
A7	3,8	76%

Tabel 9 - Variabel Kegunaan Sistem

Kode	Nilai Rata-rata	Persentase
B1	4,4	88%
B2	4,4	88%
B3	4,6	92%
B4	3,9	78%
B5	4,5	90%
B6	4,3	86%

Tabel 10 - Variabel Kemudahan Penggunaan

e-ISSN: 2548-6861

Kode	Nilai Rata-rata	Persentase
C1	4,5	90%
C2	4,4	88%
C3	4,5	90%
C4	4,5	90%
C5	4,5	90%
C6	4,6	92%

Tabel 11 - Variabel Keandalan Sistem

Kode	Nilai Rata-rata	Persentase
D1	4,7	94%
D2	4,6	92%
D3	4,6	92%
D4	4,6	92%
D5	4,7	94%
D6	4,5	90%

Tabel 12 - Variabel Kepuasan Pengguna

Berdasarkan hasil perhitungan evaluasi kuesioner UAT yang telah dilakukan, kemudian hasil tersebut dirangkum seperti pada Tabel 13.

Variabel	Nilai Bobot %	Keterangan
Kegunaan Sistem	88%	Sangat Baik
Kemudahan Penggunaan	87%	Sangat Baik
Keandalan Sistem	90%	Sangat Baik
Kepuasan Pengguna	92%	Sangat Baik

Tabel 13 - Hasil Akhir Perhitungan UAT

Dari Tabel 12 nilai hasil rata-rata setiap variabel diperoleh kesimpulan bahwa hasil interpretasi dari integrasi SIEM dan SOAR untuk otomatisasi pemblokiran IP *address* pada *router* MikroTik di PT XYZ ini termasuk dalam kategori sangat baik.

IV. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem integrasi SIEM (Wazuh) dan SOAR (Shuffle) yang terintegrasi dengan *threat intelligence* (MISP) dan *router* MikroTik untuk mengotomatisasi proses pemblokiran IP *address* berbahaya di PT XYZ. Sistem yang dibangun mampu menjalankan alur respons ancaman secara otomatis, mulai dari deteksi IoC oleh Wazuh, validasi reputasi IP *address* melalui MISP, hingga eksekusi perintah pemblokiran pada *router* MikroTik melalui API, serta pengiriman e-mail kepada Divisi IT.

Berdasarkan evaluasi menggunakan metode UAT yang melibatkan 14 responden dari seluruh anggota Divisi IT PT XYZ, seluruh variabel pengukuran memperoleh hasil dalam kategori sangat baik, yaitu kegunaan sistem sebesar 88%, kemudahan penggunaan sebesar 87%, keandalan sistem sebesar 90%, dan kepuasan pengguna sebesar 92%. Hasil ini menunjukkan bahwa sistem integrasi SIEM dan SOAR yang dibangun diterima dengan baik oleh pengguna dan dinilai efektif dalam mendukung operasional keamanan siber PT XYZ.

Meskipun demikian, sistem yang dibangun masih memiliki beberapa keterbatasan. Cakupan monitoring saat ini hanya terbatas pada server *endpoint* yang menjalankan layanan web profil dan web aplikasi PT XYZ, sehingga belum mencakup seluruh infrastruktur jaringan secara menyeluruh. Selain itu, sistem ini hanya berfokus pada pemblokiran IP *address* sebagai langkah mitigasi awal, sedangkan tindakan respons yang lebih lanjut masih bergantung pada analisis lanjutan oleh Tim SOC dan juga diharapkan Tim SOC melakukan peninjauan terjadwal untuk memastikan sistemnya tetap berjalan dengan baik.

Untuk pengembangan lebih lanjut, disarankan agar cakupan monitoring diperluas ke seluruh infrastruktur jaringan PT XYZ, tidak hanya terbatas pada server *endpoint*. Selain itu, integrasi dengan *workflow* yang lebih komprehensif pada SOAR perlu dikembangkan agar tindakan mitigasi tidak hanya sebatas pemblokiran IP *address*, tetapi juga mencakup isolasi host dan pembuatan tiket insiden secara otomatis. Peningkatan antarmuka dan dokumentasi teknis juga perlu diperhatikan guna mempermudah pengoperasian sistem bagi pengguna dengan latar belakang teknis yang beragam.

DAFTAR PUSTAKA

[1] B. A. Prasetia, D. A. Ramadhany, G. Guniawan and I. G. Waluyo, "Analisa Perangkat Fortinet Sebagai Firewall Untuk Memblokir Aplikasi Sosial Media Dan Platform Streaming Saat Jam Kerja (Studi Kasus : PT. Aplikanusa Lintasarta)," *Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia,* Vols. 1, No 3, pp. 496-504, 2023.

[2] C. K. Wilujeng and A. Voutama, "IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI FILTERING CONTENT PADA JARINGAN KOMPUTER MENGGUNAKAN MIKROTIK," *JATI (Jurnal Mahasiswa Teknik Informatika),* vol. 8 No. 3, 2024.

[3] K. M. Fern and S. Setapa, "Expert Rules of Firewall: A Technique to Construct and Modified a Set of Rules," *International Journal of Information and Education Technology,* vol. 5, 2015.

[4] B. Maris and F. Toms, "API – RouterOS – MikroTik Documentation. MikroTik," 2025.

[5] M. Al amin and R. Rahman, “IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DALAM MENINGKATKAN KEAMANAN JARINGAN,” *JURTIKOM,* vol. 1, pp. 01-05, 2024.

[6] A. O. Aljahdali and R. Alsulami, “STREAMLINING THREAT RESPONSE AND AUTOMATING CRITICAL USE CASES WITH SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR),” *Journal of Digital Security and Forensics,* vol. 2 No. 1, p. 36–57, 2025.

[7] NIST, “The NIST Cybersecurity Framework (CSF) 2.0,” 2024.

[8] V. Hugo and M. Proust, “Integrating Firewalls with SIEM and SOAR Platforms for Automated Threat Response,” *International Journal of Trend in Scientific Research and Development (IJTSRD),* vol. 6 Issue 3, 2022.

[9] S. Langrock, “What is Threat Intelligence?,” 2024.

[10] F. Ardianto and Eliza, “PENGGUNAAN MIKROTIK ROUTER SEBAGAI JARINGAN SERVER,” *Jurnal Surya Energy,* vol. 1 No. 1, 2016.

[11] A. Aliyah, N. Hartono and A. A. Muin, “Penggunaan User Acceptance Testing (UAT) Pada Pengujian Sistem Informasi Pengelolaan Keuangan Dan Inventaris Barang,” *Switch : Jurnal Sains dan Teknologi Informasi,* vol. 3 No. 2 (2025), 2025.

[12] B. Simamora, “Skala Likert, Bias Penggunaan dan Jalan Keluarnya,” *Jurnal Manajemen,* vol. 12 No. 1 (2022), 2022.

e-ISSN: 2548-6861

Appendix

Nama	A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	B5	B6	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	D5	D6
Yudista Rahadian	5	5	4	4	4	4	5	4	4	4	3	3	4	4	5	5	4	4	5	5	4	5	5	4	4
Zabal	4	4	4	4	4	5	4	4	4	4	3	4	4	3	4	3	4	3	4	5	5	5	5	5	5
Adytia	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4
Tuflikhun	5	5	5	5	4	5	5	4	4	5	4	5	5	5	5	5	5	5	5	5	5	4	5	5	4
Jovi Endar Susanto	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4
Julio Tatho	5	4	5	5	5	5	5	4	5	5	4	5	5	5	4	4	5	5	5	5	5	5	5	5	5
Ricky Nurwijayanto	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Changmato Hasibuan	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Dimas Rizky Feriyanto	4	5	5	5	5	4	4	5	5	5	3	5	5	5	4	5	5	5	5	5	4	4	4	5	5
Muhammad Arifattha	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Jovan Oldi Octorino Lukas	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Fendy Winata	5	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
Wahyu Wibowo	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Wanda	5	5	5	5	5	5	4	5	5	5	3	5	3	5	5	5	5	5	5	5	5	5	5	5	5

Tabel 14 – Hasil Kuesioner Responden