Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Perancangan Dan Implementasi *Security Information and Event Management* (SIEM) pada Layanan *Virtual Server*

Huelilik Dyan Heluka[1*], Wiwin Sulistyo[2]
Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
*e-mail *Corresponding Author*: 672016220@student.uksw.edu

Abstract

Devices accessible through the Internet have provided incredible convenience and connectivity in everyday life. However, the reality is that the device is also an attractive target for bad actors. Security threats such as malware attacks, computer virus attacks, and other cyberattacks can easily attack devices connected to the Internet. To overcome these challenges, effective and sophisticated solutions are needed. SIEM is a security platform that combines security information management (SIM) and security event management technology. (SEM). SIEM Works by collecting logs from various sources and then normalizing and aggregating log event data that is then processed using contextual parameters contained in SIEM collected from various internal and external endpoint devices such as Operating systems and network devices. The research is aimed at implementing the Wazuh SIEM with the primary objective of centralizing logs to quickly detect attacks on VPS, especially web application attacks and SSH protocol attacks. With the final results of SIEM implementation, log data from each application can be decentralized and visualized in a dashboard, and SIEM is able to detect attacks on previously undetected web applications and SSH protocols.

Keyword: *Security Operation Center; SIEM; Open Source; Wazuh;*

Abstrak

Perangkat yang dapat diakses melalui jaringan internet telah memberikan kenyamanan dan konektivitas yang luar biasa dalam kehidupan sehari-hari. Namun, kenyataannya adalah bahwa perangkat tersebut juga menjadi sasaran menarik bagi para aktor jahat. Ancaman keamanan seperti serangan malware, serangan virus komputer, dan serangan Siber lainnya dapat dengan mudah menyerang perangkat yang terhubung ke internet. Untuk mengatasi tantangan ini, diperlukan solusi yang efektif dan canggih. *Security Information and Event Management (*SIEM) merupakan platform keamanan yang menggabungkan teknologi *Security Information Management* (SIM) dan *Security Event Management* (SEM). SIEM Bekerja dengan cara mengumpulkan log dari berbagai sumber kemudian menormalisasi dan mengagregasi data peristiwa log yang kemudian diproses menggunakan parameter kontekstual yang terdapat di dalam SIEM, yang dikumpulkan dari berbagai sumber internal dan eksternal perangkat Endpoint seperti Sistem Operasi, kontainer, dan perangkat jaringan. Penelitian ini bertujuan untuk mengimplementasikan SIEM Wazuh dengan tujuan utama yaitu melakukan sentralisasi log untuk mendeteksi dengan cepat serangan pada VPS, terutama pada serangan aplikasi web dan serangan pada protokol SSH. Dengan hasil akhir implementasi SIEM, data log dari setiap aplikasi dapat disentralisasi dan divisualisasikan dalam sebuah dashboard, serta SIEM mampu mendeteksi serangan pada aplikasi web dan protokol SSH yang sebelumnya tidak terdeteksi.

Kata kunci: *Security Operation Center; SIEM; Open Source; Wazuh;*

1. Pendahuluan

Teknologi informasi pada bidang komputer terus mengalami perkembangan yang pesat mulai dari perangkat lunak hingga perangkat keras. Salah satu perkembangan yang diadopsi oleh suatu organisasi saat ini yaitu teknologi virtualisasi. Virtualisasi memungkinkan satu sistem fisik dibagi menjadi beberapa sistem yang sebut juga *virtual server* yang dapat menjalankan aplikasi atau sistem operasi yang berbeda secara independen, layanan virtualisasi juga di

komersilkan dalam bentuk *virtual private server* (VPS). Dinas Komunikasi Dan Informatika Kota Salatiga (DISKOMINFO) merupakan salah satu organisasi pemerintahan yang menerapkan layanan virtualisasi. Hadirnya teknologi ini ini mampu menghemat biaya yang dikeluarkan pada saat membangun *server* [1]. Organisasi cukup membeli atau menyewa *server* kemudian menjalankan virtualisasi sehingga diperoleh beberapa virtual *server*. Dengan seiring perkembangan organisasi dan jumlah virtual *server*, maka diperlukan sistem yang mampu memantau aktivitas *server*.

Kejadian serangan siber pada *server* seringkali tidak disadari oleh administrator. Berdasarkan data yang dikumpulkan melalui wawancara dan pemeriksaan *log* pada *server* serta aplikasi *web server*, terdapat beragam jenis serangan yang menargetkan perangkat yang dimiliki oleh Diskominfo, serangan-serangan tersebut berhasil melewati *firewall* dan melakukan direspon oleh server, yang di dominasi oleh serangan *ssh password guessing*, dan *directory scanning.* peristiwa yang paling signifikan terjadi menjelang akhir tahun 2022, yang mengakibatkan *subdomain* tidak dapat diakses dan data cadangan yang disimpan di *server* yang sama terhapus, Insiden berbahaya biasanya di deteksi dengan menganalisis log, namun untuk beberapa serangan lebih kompleks analisis log saja belum tentu dapat mendeteksi adanya insiden ini, dan hal yang sama pula dapat terjadi jika seorang administrator sistem mengabaikan analisis *log* pada system [2]. Untuk mengatasi permasalahan serupa, diperlukan sebuah sistem deteksi serangan yang dapat memberikan informasi secara *real-time* tentang keadaan *server* saat terjadi serangan. Agar seorang administrator dapat dengan cepat dan tepat mengambil langkah-langkah preventif untuk melindungi perangkat *server*.

Security Information and Event Management (SIEM) adalah sebuah sistem monitoring dan analisis keamanan yang bekerja secara *real-time* ataupun melalui history log yang bertujuan untuk mengumpulkan berbagai aktivitas log dari host system, dengan tujuan untuk mengidentifikasi kemungkinan terjadinya serangan pada *host system* [3]. Selain itu, sistem ini didesain untuk menganalisis setiap peristiwa keamanan yang terjadi pada perangkat jaringan dan aplikasi secara *real-time*, dan memberikan respons terhadap ancaman tersebut sebelum terjadi serta mencegah terjadinya kerusakan yang signifikan [4]. Wazuh *Endpoint Security* merupakan perangkat lunak berbasis *Open Source Security Platform* yang memiliki fungsi sebagai *Security Information and Event Management* (SIEM) yang dapat berjalan pada sistem operasi Windows, Linux, dan MacOS. Wazuh *server* merupakan tempat dikumpulkanya *log* dari *endpoint host sistem* yang setiap saat dikirimkan oleh Wazuh *agent* untuk kemudian dianalisis dan dicocokkan dengan database Wazuh server secara otomatis untuk kemudian diidentifikasi apakah merupakan aktivitas normal atau abnormal [5].

Penelitian ini bertujuan untuk membuktikan SIEM dengan nama wazuh dapat melakukan pemantauan *server* secara terpusat dengan efektif pada perangkat diskominfo. Selain itu penelitian ini juga akan melakukan implementasi SIEM wazuh pada DISKOMINFO Kota salatiga, serta melakukan pengujian serangan kepada *host server.*

2. Tinjauan Pustaka

Dalam penelitian yang berjudul [6] membahas tentang urgensi menjaga keamanan lingkungan jaringan dari serangan aktor jahat yang menargetkan sistem dan data yang ada di dalam jaringan. Alat yang digunakan untuk pendeteksian adalah *honeypot* yang diintegrasikan dengan IDS berbasis *host*, untuk mengetahui teknik dan taktik penyerang maka di pasanglah perangkap *honeypot* yang dihubungkan dengan IDS untuk menganalisa serangan yang terjadi pada *honeypot.* Hasil analisa menunjukan tipe serangan ssh *brute force attack* merupakan serangan yang kerap terjadi pada *honeypot*.

Pada penelitian yang berjudul [7] penulis merancang sistem keamanan dan menggunakan *honeypot* sebagai jebakan bagi aktor jahat serta menggabungkan HIDS dengan nama Wazuh untuk menguji sejauh mana kemampuan HIDS ini mendeteksi serangan yang terjadi. Dengan hasil HIDS efektif memantau aktifitas serangan yang terjadi.

Berdasarkan Penelitian Yang berjudul [8] Menjelaskan bahwa IDS yang dikombinasikan dengan SIEM dapat mendeteksi anomali secara real time. Dalam penggunaannya dilakukan serangan DoS dengan jumlah paket per detik nya sebanyak 344 paket selama satu jam, yang mengakibatkan lonjakan proses pada CPU dan RAM. Semua proses ini dapat di monitoring secara real-time melalui SIEM.

Dalam penelitian selanjutnya dengan judul [9] melakukan pengujian SIEM wazuh yang sudah terpasang pada *server web* Universitas Beograd. Agen wazuh yang telah terpasang pada

perangkat *server web* secara *real-time* melakukan pemindaian dengan menggunakan berbagai modul yang ada di dalam SIEM Wazuh diantaranya ada *Security Configuration Assessment, Auditing dan Policy Monitoring.* Hasil pengujian tersebut memberikan wawasan yang menyeluruh tentang keamanan sistem dan langkah preventif untuk mengamankan *server web* kepada administrator Universitas Beograd.

Dalam penelitian yang berjudul [10] membahas tentang pentingnya penerapan SIEM pada perangkat IOT. SIEM merupakan solusi yang baik bagi keamanan pemantauan jarak jauh. pada penelitian ini sepenuhnya agent tidak di pasang pada *endpoint* perangkat IOT. Penelitian ini mengusulkan skema pemantauan trafik jaringan pada perangkat IOT menggunakan Tools Wazuh yang berjalan tanpa agent, yang mana trafik jaringan pada *gateway* perangkat IOT akan didokumentasikan dan dikumpulkan yang kemudian masuk ke dalam proses analisa pada SIEM dengan nama wazuh.

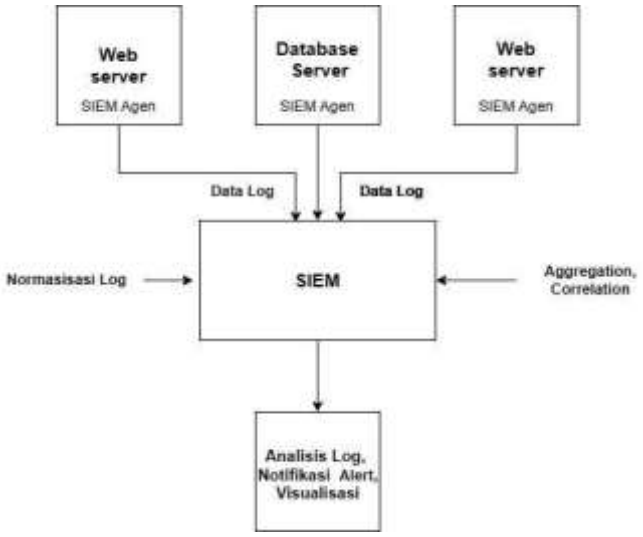
Penelitian ini berbeda dengan beberapa penelitian sebelumnya. Penelitian kali ini akan melakukan Implementasi SIEM bernama Wazuh pada lingkup Dinas Komunikasi dan Informatika Kota salatiga untuk mendeteksi adanya serangan yang berupa serangan *Web attack* dan serangan *brute force ssh* yang mengarah ke perangkat endpoint berupa server yang dimiliki organisasi.

3. Metodologi

Dalam perancangan dan implementasi security information and event management (SIEM) untuk mendeteksi adanya serangan pada VPS khusus nya serangan pada web aplikasi dan protokol ssh, digunakan perangkat bernama Wazuh, Wazuh sendiri merupakan perangkat yang kaya akan fitur untuk mendeteksi ancaman pada makalah yang berjudul [9] menjelaskan kemampuan wazuh mendeteksi serangan pada sebuah honeypot dan dapat di padu padankan dengan pembelajaran mesin sehingga mampu mendeteksi dan merespon serangan siber yang terjadi secara tepat. Perancangan ini diperlukan karena dalam penerapan SIEM juga diperlukan analisis dan perencanaan yang terstruktur sebelum dilakukan implementasi [15].

3.1. Arsitektur SIEM

Security Information And Event Management (SIEM) Merupakan Kumpulan komponen atau modul yang bekerja untuk mencapai tujuan nya [11]. SIEM sendiri pertama kali dikenalkan oleh Gartner coined pada tahun 2005 yang merupakan gabungan dari dua perangkat yang sebelumnya terpisah yaitu (SEM) Security Event management dan (SIM) Security Information management SIEM bekerja dengan cara mengumpulkan setiap log event dari suatu proses [4]. Kemudian, dilakukan pencatatan peristiwa, normalisasi, agregasi, dan korelasi peristiwa.



Gambar 1. Arsitektur SIEM

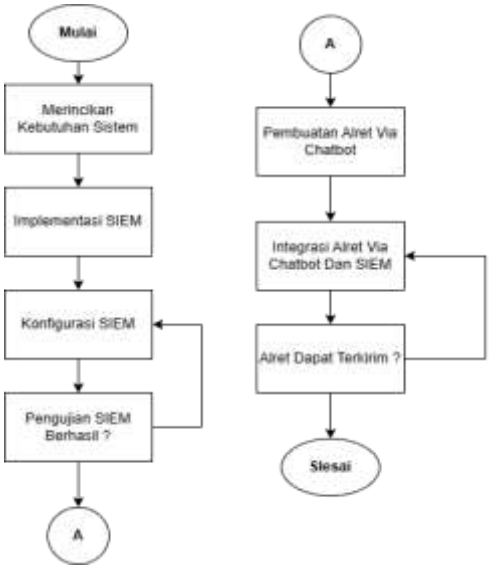
Dalam tahap pencatatan, SIEM menyimpan data yang dikumpulkan dan diteruskan oleh agen pada perangkat. Data ini dikumpulkan dari berbagai jenis perangkat dan diubah ke dalam format

yang dikenali sistem, sehingga operasi pengolahan data dapat dilakukan dengan efektif. Setelah normalisasi, indikator yang tidak perlu dari log event dieliminasi melalui proses agregasi. Selanjutnya, log event yang telah diproses dikorelasikan untuk mendeteksi perilaku mencurigakan dan pola yang tidak diketahui. Setelah semua fungsi tersebut dilakukan pada data yang dikumpulkan, solusi SIEM akan menghasilkan Visualisasi dan peringatan jika terdeteksi adanya aktivitas yang dianggap tidak normal pada perangkat. Pada gambar 1 dibawah merupakan gambaran tiap proses dalam SIEM.

4. Hasil dan Pembahasan

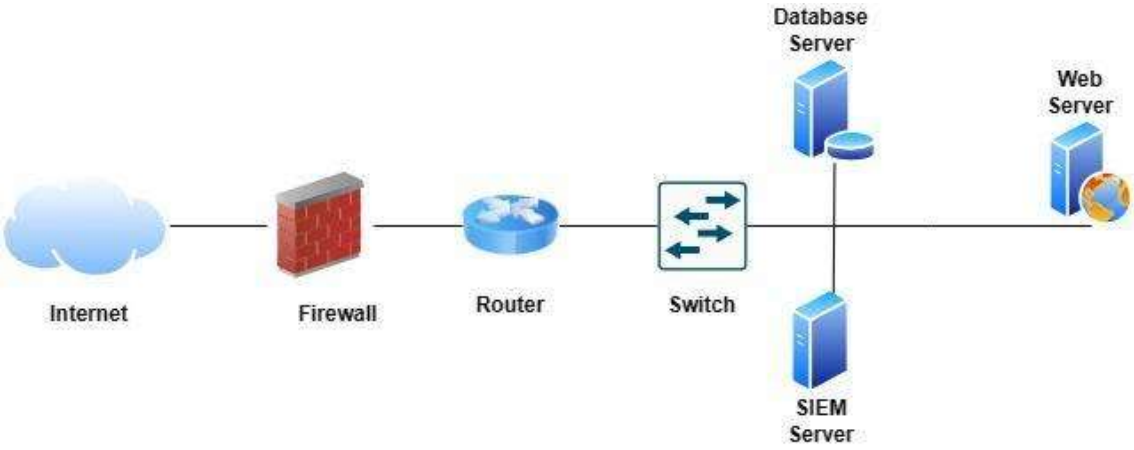
4.1 Perancangan

Pada tahap ini dilakukan perancangan SIEM Wazuh dengan merincikan alur implementasi, Topologi SIEM dan, mendeskripsikan spesifikasi Perangkat Yang digunakan. Dalam penelitian ini perancangan dibagi menjadi 2 bagian perancangan SIEM dan perancangan alert SIEM sebagai alat pengiriman notifikasi untuk pemantauan mobile.



Gambar 2. Diagram Alir Perancangan SIEM Wazuh dan Alert

Alur pada gambar 2 menjelaskan tentang proses perancangan sistem. dengan menggunakan diagram alir yang disesuaikan dengan tiap elemen di dalamnya merepresentasikan proses instalasi yang dimulai dengan pemasangan SIEM Wazuh pada server dan agent pada *server endpoint*. Server wazuh terhubung pula dengan chabot telegram melalui api dari telegram, yang mempermudah pengiriman notifikasi alert.



Gambar 3. Topologi SIEM

`

Dalam topologi yang dilampirkan pada gambar 3, dapat terlihat *server* SIEM yang terhubung dengan internet terhubung pula dengan server siem, yang nantinya saat terjadi request ke *server* web atau *database* tiap *log* nya akan di teruskan ke server SIEM untuk di proses.

Pada perancangan ini akan di rincikan perangkat yang akan digunakan dalam penelitian, tabel 1 menunjukan perangkat keras yang akan digunakan dan tabel 2 merupakan komponen perangkat lunak SIEM yang diimplementasikan. Spesifikasi perangkat yang digunakan dalam penelitian ini adalah sebagai berikut:

Tabel 1. Spesifikasi Perangkat Keras

Nama Perangkat Keras	Spesifikasi
Server SIEM Wazuh	OS Debian 1
	Ram 8GB
	Penyimpanan HDD 512 GB
Server Agent	OS Ubuntu 18.04
	Ram 4 GB
	Penyimpanan 480GB SSD

Tabel 2. Spesifikasi Perangkat Lunak

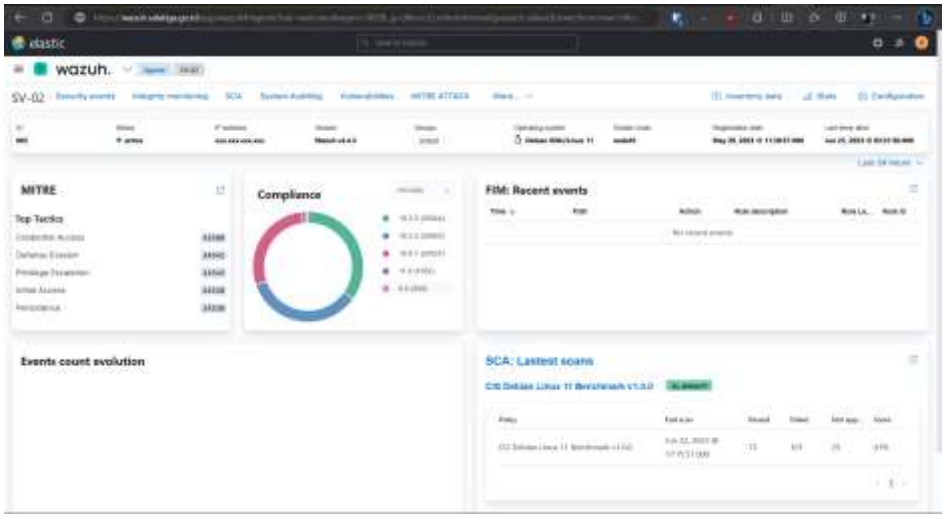
Nama Perangkat Lunak	Spesifikasi
SIEM Wazuh	Versi 4.4.0
Wazuh Agent	4.4.0
Elasticsearch	7.17.9
Filebeat	7.17.9
Kibana	7.17.9
Bot API	6.7

4.2. Implementasi

Gambar 3 Proses Pemasangan SIEM Wazuh

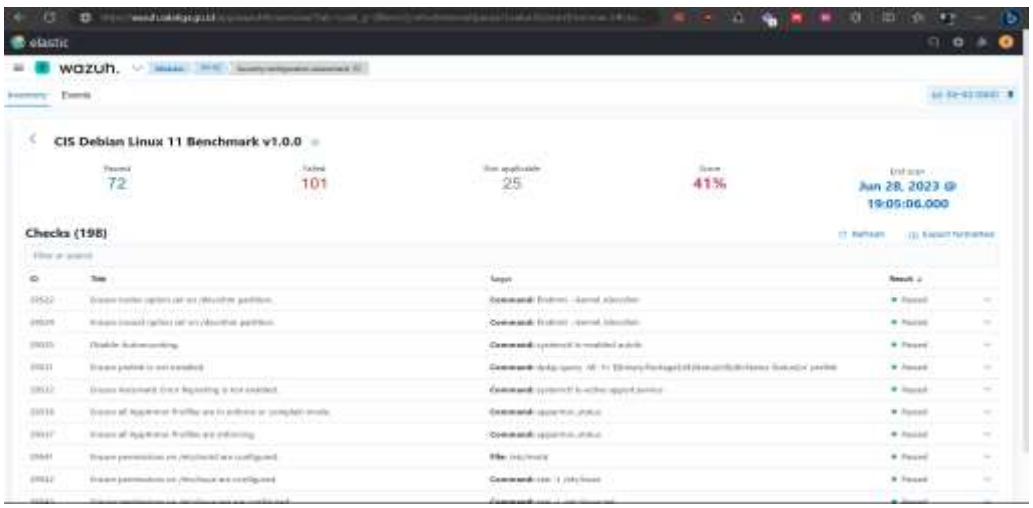
Implementasi adalah tahap yang dilakukan setelah tahap perancangan atau desain yang dibuat diwujudkan menjadi suatu sistem yang utuh dan dapat digunakan. Implementasi dalam penelitian ini dibagi menjadi 2 bagian Implementasi SIEM dan Implementasi Notifikasi alert.

Dalam tahap implementasi, akan dilakukan *instalasi* SIEM Wazuh pada *server* lokal milik Dinas Komunikasi dan Informatika Kota Salatiga. Gambar 3 menunjukan proses pemasangan telah berhasil, dikarenakan pemasangan menggunakan bantuan script bash maka secara default username dan password login dari SIEM akan *tergenerate* otomatis dan dapat dilakukan penggantian pula.



Gambar 4 Tampilan agent SIEM Wazuh

Server siem yang telah terinstall tidak langsung terhubung ke *agent* atau *host endpoint*, diperlukan pemasangan dengan agent agar agent host dapat terhubung dan mengirimkan status *server*, pada gambar 4 merupakan *virtual private server* yang di dalam nya telah terpasang agent dari wazuh dan telah aktif mengirimkan kondisi *server* secara *real-time* ke *server* SIEM Wazuh. Agent yang terhubung pertama kali ke SIEM Wazuh akan dipindai menggunakan fungsi *Aggregation* dan *Correlation* untuk menemukan hubungan dari data yang[12].Selanjutnya, data tersebut akan dicocokkan dengan indikator yang dimiliki oleh CIS *benchmark* guna melihat kesesuaian dengan standar keamanan yang ditetapkan. Selanjutnya, SIEM Wazuh akan memberikan laporan dan rekomendasi berdasarkan hasil pemindaian tersebut, hasil pemindian dapat di lihat pada gambar 5.



Gambar 5 Hasil benchmark agent

4.3. Analisis Log Serangan

Pada langkah ini penulis akan melakukan analisis pada sistem yang telah diimplementasikan, analisis ini meliputi pendeteksian serangan pada *web server* dan serangan pada ssh protokol yang terdapat di dalam agent *virtual private server* (vps) yang telah di daftarkan ke dalam SIEM Wazuh, dikarenakan perangkat vps terhubung ke internet dan dapat diakses secara publik maka keseluruhan hasil serangan ini merupakan serangan nyata yang terjadi dan menargetkan vps milik Diskominfo.

Waktu	Rule.level	Rule.id	Alamat.IP	HTTP Response	Payload	Negara
Jun 15, 2023 @ 01:07:09.111	5	31101	45.137.206.143	405	check.best-proxies.ru:443	United State s
Jun 17, 2023 @ 03:39:02.663	5	31101	45.137.206.143	405	check.best-proxies.ru:443	United State s
Jun 15, 2023 @ 10:32:15.697	5	31101	45.137.206.143	405	checkip.amazonaws.com:443	United State s
Jun 14, 2023 @ 08:14:25.530	5	31101	45.137.206.143	405	eth0.me:443	United State s
Jun 15, 2023 @ 00:45:45.567	5	31101	45.137.206.143	405	google.com:443	United State s
Jun 16, 2023 @ 07:34:08.258	5	31101	45.137.206.143	405	google.com:443	United State s
Jun 17, 2023 @ 10:53:09.594	5	31101	45.137.206.143	405	google.com:443	United State s
Jun 13, 2023 @ 15:36:34.273	5	31101	90.151.171.188	405	v4.ident.me:443	Russia
Jun 13, 2023 @ 09:16:58.569	5	31101	161.35.206.236	403	/!.gitignore	Germany
Jun 14, 2023 @ 08:39:37.102	5	31101	161.35.206.236	403	/!.gitignore	Germany

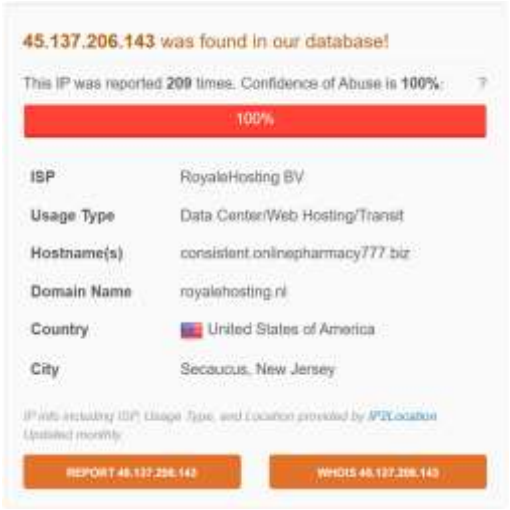
Gambar 5 Log serangan dari web server

Pada gambar 5 terlihat serangan yang terjadi dilakukan oleh berbagai penyerang yang menggunakan berbagai IP publik menggunakan *payload* yang berbagai macam dengan tujuan mendapatkan akses ke *server*. Untuk memastikan bahwa benar peretas mencoba melakukan akses kepada server maka dilakukan pengecekan pula dengan melihat log pada web server pada Gambar 6. Pada pengecekan tersebut terdapat alamat IP yang kerap melakukan request yang aneh, Dapat dilihat pula IP dengan alamat 45.137.206.143 melakukan *request* dengan metode connect yang terus berulang menggunakan berbagai parameter.

```
45.137.206.143 - - [11/Jun/2023:09:20:26 +0000] "CONNECT google.com:443 HTTP/1.1" 405
45.137.206.143 - - [11/Jun/2023:09:20:35 +0000] "CONNECT www.google.es:443 HTTP/1.1" 4
45.137.206.143 - - [11Jun/2023:09:20:47 +0000] "CONNECT google.com:443 HTTP/1.1" 405 5
```

Gambar 6 Log web server

Untuk memastikan bahawa alamat IP tersebut merupakan alamat IP dari aktor jahat, maka dilakukan pula pengecekan menggunakan database AbuseIPDB dari alamat IP tersebut, AbuseIPDB Proyek ini memiliki fokus utama dalam membantu memerangi penyebaran malware, spam, dan perilaku tidak normal dengan mengumpulkannya ke dalam sebuah sentralisasi basis data blacklist IP. Basis data ini akan memberikan bantuan kepada pemilik sistem untuk menangani masalah yang timbul dari alamat IP yang tercatat di dalamnya[13]. Pada hasil pencocokan yang dilakukan dengan basis data milik AbuseIPDB Pada Gambar 7 alamat tersebut dapat dilihat bahwa alamat Ip tersebut dilaporkan sebanyak 209 kali, dari informasi tersebut dapat diasumsikan alamat IP tersebut merupakan alamat yang dimiliki aktor jahat yang digunakan untuk kegiatan yang tidak semestinya.



Gambar 7 Pengecekan menggunakan AbuseIPDB

Analisis selanjutnya dengan melakukan pengecekan aktivitas protokol ssh pada dashboard SIEM dapat dilihat pada Gambar 8.

Waktu	Rule.Mitre.Technique	Alamat.IP	Port	Payload	Rule.ID
Jun 21, 2023 @ 20:17:11.661	Password Guessing, SSH, Valid Accounts	220.80.74.79	47991	telnet	5710
Jun 21, 2023 @ 20:17:03.653	Brute Force	118.45.164.195	33997	pi	5758
Jun 21, 2023 @ 20:17:01.661	Brute Force	220.80.74.79	47926	admin	5758
Jun 21, 2023 @ 20:16:53.642	Brute Force	220.80.74.79	47847	ubnt	5758
Jun 21, 2023 @ 20:16:43.631	Brute Force	118.45.164.195	33913	remotessh	5758
Jun 21, 2023 @ 20:16:39.627	Password Guessing, SSH, Valid Accounts	220.80.74.79	47757	telnet	5710
Jun 21, 2023 @ 20:16:31.629	Password Guessing, SSH, Valid Accounts	118.45.164.195	33810	admin	5710
Jun 21, 2023 @ 20:16:31.618	Brute Force	220.80.74.79	47685	usr	5712
Jun 21, 2023 @ 20:16:17.601	Password Guessing, SSH, Valid Accounts	220.80.74.79	47589	usr	5710
Jun 21, 2023 @ 20:16:11.595	Password Guessing, SSH, Valid Accounts	118.45.164.195	33686	ubnt	5710
Jun 21, 2023 @ 20:16:03.586	Password Guessing, SSH, Valid Accounts	220.80.74.79	47481	admin	5710
Jun 21, 2023 @ 20:15:55.583	Brute Force	118.45.164.195	33593	remotessh	5758
Jun 21, 2023 @ 20:15:49.576	Password Guessing, SSH, Valid Accounts	220.80.74.79	47405	pi	5710
Jun 21, 2023 @ 20:15:39.566	Password Guessing, SSH, Valid Accounts	220.80.74.79	47327	telnet	5710

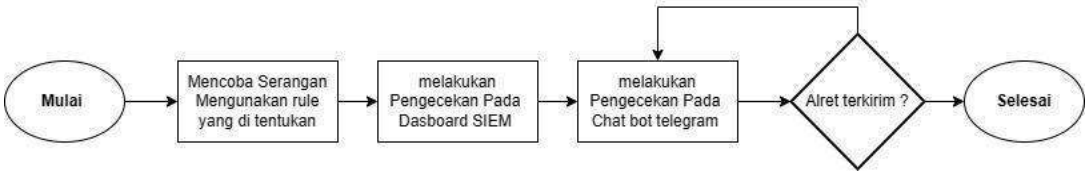
Gambar 8 dashboard SIEM

Pada beberapa perangkat yang dimiliki Diskominfo menggunakan protokol SSH untuk melakukan remote jarak jauh pada perangkat nya, ini menjadi suatu celah yang cukup rawan meskipun pada level jaringan telah memiliki Firewall seperti ditunjukkan pada Gambar 3. Namun aktor jahat mencoba melakukan *bypass* dengan mengubah frekuensi serangan agar tidak terdeteksi oleh *firewall* dan penggunaan IP yang berbeda beda untuk melewati rule pada firewall. SIEM Wazuh dapat mendeteksi aktifitas tersebut, Gambar 8 menunjukan adanya percobaan login menggunakan nama pengguna yang berbeda dan port yang berbeda, dan penyerang terlihat membatasi jumlah percobaan hanya dua kali tiap beberapa saat dan mengubah alamat IP lain untuk melakukan serangan selanjutnya berulang dan silih berganti.

Pada SIEM Wazuh data serangan yang diperoleh dari log dapat divisualisasikan pula pada SIEM Wazuh untuk mengetahui lokasi mana saja yang paling sering melakukan Serangan SSH dan Serangan Web yang terdeteksi.

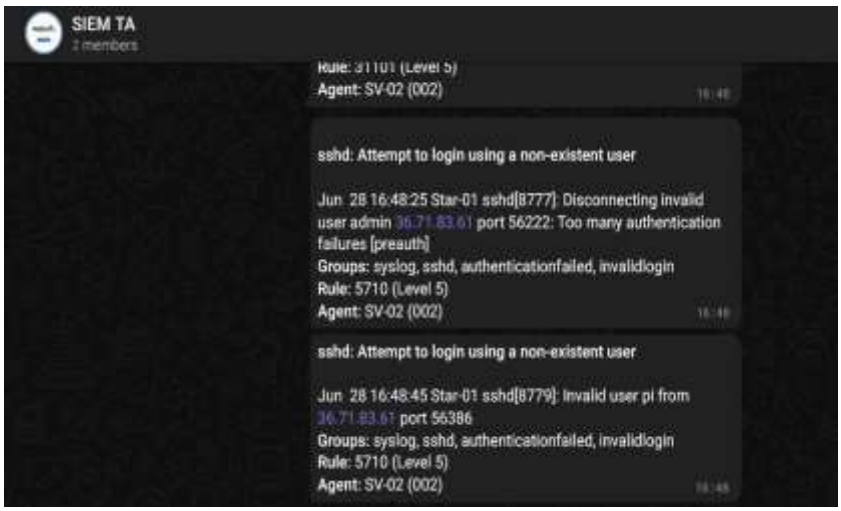
Gambar 9 Visualisasi lokasi serangan

4.4. Pengujian Notifikasi Serangan

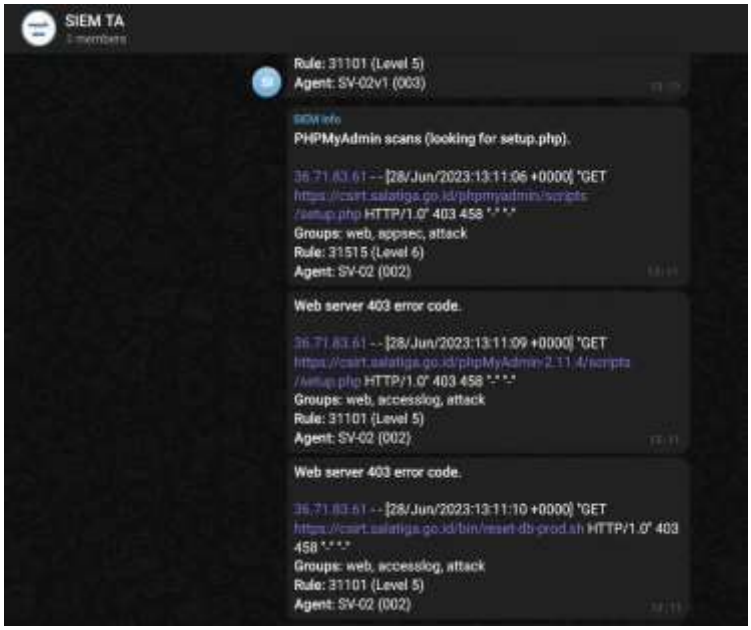


Gambar 10 Serangan

Untuk mempermudah administrator sistem maka dibuatlah notifikasi serangan menggunakan chatbot telegram untuk mengirimkan notifikasi ketika serangan terjadi secara realtime, notifikasi pada telegram dibatasi hanya alert level 5 keatas yang akan diteruskan menggunakan chatbot agar tidak memenuhi ruang chat dan membuat administrator kebingungan. Pengujian serangan ke server web tidak dilakukan dengan menggunakan alat automasi melainkan menggunakan request manual ke server web, tujuannya agar server web tidak kewalahan memproses permintaan yang terjadi. begitu pula pada serangan ssh akan di lakukan secara manual dengan mencoba port login yang berbeda dan nama pengguna yang berbeda, Pengujian ini dilakukan serangan langsung web attack dan ssh attack pada server Diskominfo Kota Salatiga.



Gambar 11 Notifikasi Alert ssh attack



Gambar 11 Notifikasi Alert Web Attack

Serangan yang berhasil terdeteksi oleh SIEM akan langsung diteruskan melalui api *chatbot* telegram ke ruang chat, yang dapat di lihat pada gambar 11 dan gambar 12, data informasi mengenai waktu, payload, dan server yang di serang dapat di lihat langsung pada ruang chat telegram.

Untuk menguji keefektifan SIEM maka dilakukan Uji monitoring yang dilakukan selama 3 bulan dalam pengujian yang dilakukan selama 3 bulan ini monitoring hanya difokuskan pada dua tipe serangan yaitu Serangan Web dan Serangan Protokol SSH yang dapat dilihat pada Tabel 3.

Tabel 3 Uji Monitoring

Jenis Serangan	Bulan ke 1	Bulan ke 2	Bulan ke 3
Serangan Web	8.034	6.435	6.843
Serangan SSH	11.646	10.323	12.056

Untuk menguji keefektifan SIEM maka dilakukan Uji monitoring yang dilakukan selama 3 bulan dalam pengujian yang dilakukan selama 3 bulan ini monitoring hanya difokuskan pada dua tipe serangan yaitu Serangan Web dan Serangan Protokol SSH yang dapat dilihat pada Tabel 3. Dengan adanya implementasi SIEM dengan nama Wazuh ini akan mempermudah seorang administrator dalam hal merespon dan mengetahui keadaan sistem yang dimilikinya secara terpusat [2]. Penelitian ini mendukung pendapat dari penelitian yang terdahulu dengan dudul [9],[6] yang mengatakan SIEM dengan Nama Wazuh ampuh dan dapat dideteksi sebagai jenis serangan dengan efektif dan dengan ada nya siem dapat memberikan gambaran kondisi aset secara realtime. perangkat firewall jaringan saja tidak cukup untuk mengamankan perangkat endpoint namun diperlukan pula perangkat yang mampu mendeteksi jejak aktifitas melalui log, dan SIEM merupakan Solusi yang efektif [14] Hasil Implementasi pada lingkungan production SIEM ini terbukti efektif mendeteksi serangan pada Level web aplikasi dan serangan pada protokol ssh yang berhasil melewati firewall level jaringan. dalam hasil uji monitoring selama 3 bulan terhitung sejak SIEM diImplementasikan sebanyak 21.312 Serangan pada web App dan 34.025 serangan pada protokol ssh yang berhasil tak terdeteksi.

5. Simpulan

Berdasarkan penelitian mengenai Perancangan dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server, dapat disimpulkan bahwa penerapan perangkat SIEM dengan nama Wazuh telah berhasil mencapai tujuan utamanya. Perangkat SIEM ini mampu melakukan pemantauan log secara terpusat dengan efektif, sehingga memangkas waktu deteksi dan respon dari administrator saat terjadi insiden keamanan.Dalam implementasi ini, keterlibatan aktif dan berkesinambungan oleh administrator sistem, serta tim keamanan pada organisasi, sangat diperlukan untuk merancang aturan yang terus diperbarui pada SIEM. Pada penelitianberikutnya dapat dilakukan dengan mengembangkan integrasi SIEM dengan perangkat jaringan seperti firewall untuk memantau lalu lintas keluar dan masuk yang mencurigakan. Hal ini bertujuan agar tindakan pengamanan yang sesuai dapat dilakukan dengan lebih tepat dan efisien.

Daftar Referensi

[1] J. Nie, “A study on the application cost of server virtualisation,” in *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 2013, pp. 807–811. doi: 10.1109/CIS.2013.176.

[2] Bojana Vilendečić, Ratko Dejanović, and Predrag Ćurić, “The Impact of Human Factors in the Implementation of SIEM Systems,” *J. of Electrical Engineering*, vol. 5, no. 4, Jul. 2017, doi: 10.17265/2328-2223/2017.04.004.

[3] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, “Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures,” *Sensors*, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144759.

[4] IBM,“What is Security Information and Event Management (SIEM)? ” IBM, 2022, [Online]. https://www.ibm.com/id-en/topics/siem [Diakses 18 Januari 2023].

[5] Wasuh,“Wazuh documentation.”Wazuh, 2023, [Online]. Tersedia: https://documentation.wazuh.com/current/index.html [Diakses: Desember 14 2022].

[6] M. . Hafiz and B. . Soewito, “Information Security Systems Design Using SIEM, SOAR and Honeypot”, *jptam*, vol. 6, no. 2, pp. 15913–15926, Jul. 2022, doi: 10.31004/jptam.v6i2.4898.

[7] R. M. Muhammad, I. Dyah Irawati, and M. Iqbal, “Integrated Security System Implementation for Network Intrusion,”*Journal of Hunan University (Natural Sciences).,* Vol.48, No.6, June 2021.

[8] Muhammad Adabi Raihan, “Sistem Security Information & Event Management (SIEM) untuk Live Analysis berbasis Machine Learning pada Intrusion Detection System (IDS),”e-Proceeding of Engineering., Vol.9, No.4, p.1985 2022.

[9] S. G. P. Stefan Stankovic, “A Review Of Wazuh ToolCapabilities for Detecting Attacks Based on Log Analysis,” Proceedings, Ix International Conference Icetran, Novi Pazar, Serbia, 6 - 9. june 2022.

[10] H. Zahid, S. Hina, M. F. Hayat, and G. A. Shah, “Agentless Approach for Security Information and Event Management in Industrial IoT,” Electronics, vol. 12, no. 8, p. 1831, Apr. 2023, doi: 10.3390/electronics12081831.

[11] M. Sheeraz *et al.*, “Effective Security Monitoring Using Efficient SIEM Architecture,” *Human-centric Computing and Information Sciences*, vol. 13, p. 17, 2023, doi: 10.22967/HCIS.2023.13.017.

[12] K. Kent dan M. Souppaya, “Guide to Computer Security Log Management,” NIST SP 800-92, 13 September 2006, doi: 10.6028/NIST.SP.800-92. Kent and M. Souppaya, “Special Publication 800-92 Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology.” , doi: 10.6028/NIST.SP.800-92

[13] AbuseIPDB, “AbuseIPDB - IP address abuse reports,”AbuseIPDB, 2023. [Online]. Tersedia: https://.abuseipdb.com [Diakses:January 25, 2023].

[14] Avira, “What is a SIEM? Definition & Explanation.”, Avira, 9 February 2023, [Online]. Tersedia: https://www.avira.com/en/blog/your-beginners-guide-security-information-and-event-management-siem [Diakses: 5 Maret 2023].

[15] Miller, D. R., Harris, S., Harper, A. A., VanDyke, S., & Blask, C. Security Information and Event Management (SIEM) Implementation. New YorkNew York: McGraw-Hill.2010.