



**LAPORAN AKHIR  
PROJECT BASED LEARNING  
SIEM Development and Game-Based Security Operation  
Center (SOC) Simulation Blue Team-412**



**PROGRAM STUDI REKAYASA KEAMANAN SIBER  
JURUSAN TEKNIK INFORMATIKA  
POLITEKNIK NEGERI BATAM  
2025**

## Identitas Proyek

Judul Proyek : SIEM Development and Game-Based Security Operation  
Center (SOC) Simulation Blue Team-412

Pengusul Proyek : Maidel Fani, S.Pd., M.Kom.

Manager Proyek : Agus Fatulloh, S.T., M.T

Co-Manajer Proyek : -

Klien : Politeknik Negeri Batam

Luaran : 1. Laporan Akhir  
2. Video Presentasi dan Demo  
3. Poster

Tim PBL:

No	Nama	Nim	Prodi	Pembagian Tugas
1.	Rey Sastria Harianja (Team Leader)	4332301038	Rekayasa Keamanan Siber	<ul style="list-style-type: none"><li>• Membuat Web Aplikasi</li><li>• Membbackup Web Aplikasi</li><li>• Mendesain Web Aplikasi</li></ul>
2.	Akyasa Fikri Ramadhan	4332301055	Rekayasa Keamanan Siber	<ul style="list-style-type: none"><li>• Pentester</li><li>• Instalasi, konfigurasi, dan pemeliharaan sistem Wazuh, Grafana, The Hive, Cortex</li></ul>
3.	Hasbi Hakim	4332311041	Rekayasa Keamanan Siber	<ul style="list-style-type: none"><li>• Menyiapkan database utama dan database backup</li></ul>
4.	Desty Silva Dewi	4332301057	Rekayasa Keamanan Siber	<ul style="list-style-type: none"><li>• Menyusun laporan akhir, manual book dan mengumpulkan dokumentasi</li></ul>
5.	Adhitya Pramadhan	4332311044	Rekayasa Keamanan Siber	<ul style="list-style-type: none"><li>• Mengelola konfigurasi, menjalankan,</li></ul>

				dan memelihara server aplikasi.
6.	Nohiro Hazel Nayottama R.H	4332311011	Rekayasa Keamanan Siber	<ul style="list-style-type: none"> <li>• Pentester</li> <li>• Konfigurasi jaringan dan implementasi IDS/IPS dan VPN</li> </ul>

## Kata Pengantar

Puji dan Syukur kami panjatkan kepada Tuhan Yang Maha Esa atas Anugrahnya yang berlimpah, sehingga pada kesempatan kali ini kami dapat menyusun dan menyelesaikan Project Based Learning (PBL) di semester 4 ini yang berjudul “SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team-412” yang merupakan salah satu syarat untuk Ujian Akhir Semester pada Program Studi Rekayasa Keamanan Siber di Politeknik Negeri Batam.

Penyusunan Laporan Project Based Learning (PBL) ini dibantu juga dari berbagai pihak. Dalam kesempatan ini kami ingin berterimakasih kepada :

1. Bapak Agus Fatulloh, S.T., M.T selaku manager Project Based Learning
2. Ibu Maidel Fani, S.Pd., M.Kom selaku Kaprodi Rekayasa Keamanan Siber
3. Seluruh dosen Program Studi Rekayasa Keamanan Siber Politeknik Negeri Batam terimakasih atas kerjasama dan bantuannya dalam memberikan bimbingan dan arahnya.
4. Dan juga anggota kelompok.

Dalam penyusunan laporan ini, kami menyadari bahwa hasil laporan ini masih jauh dari kata sempurna dikarenakan terbatasnya pengalaman dan dan pengetahuan yang kami miliki, Oleh karena itu kami mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak. Akhirnya kami berharap semoga laporan ini dapat memberikan manfaat bagi penulis dan pembaca.

## Daftar Isi

<b>Identitas Proyek .....</b>	<b>2</b>
<b>Daftar Isi .....</b>	<b>4</b>
<b>Daftar Gambar .....</b>	<b>4</b>
<b>Daftar Lampiran .....</b>	<b>4</b>
<b>Latar Belakang .....</b>	<b>5</b>
<b>Kajian Pustaka .....</b>	<b>6</b>
<b>Perancangan .....</b>	<b>6</b>
A. <b>Deskripsi Produk .....</b>	<b>6</b>
B. <b>Rancangan Topologi dan Desain .....</b>	<b>7</b>
<b>Implementasi Produk .....</b>	<b>10</b>
<b>Future Work .....</b>	<b>15</b>
<b>Lampiran .....</b>	<b>16</b>

## Daftar Gambar

Gambar 1.1 Rancangan Topologi .....	10
Gambar 1.2 SIEM .....	10
Gambar 1.3 Firewall .....	10
Gambar 1.4 Web Server .....	10
Gambar 1.5 Database Server .....	10
Gambar 1.6 Database Backup .....	10

## Daftar Lampiran

Lampiran 1 Link Demo Project .....	<b>Error! Bookmark not defined.</b>
Lampiran 2 Poster .....	<b>Error! Bookmark not defined.</b>
Lampiran 3 Logbook .....	<b>Error! Bookmark not defined.</b>

## Latar Belakang

Di era digital saat ini, internet dan jaringan komputer telah menjadi tulang punggung berbagai sektor, termasuk pendidikan, bisnis, dan pemerintahan. Namun, seiring dengan meningkatnya ketergantungan pada teknologi, ancaman keamanan siber juga meningkat secara signifikan. Organisasi dari berbagai skala menghadapi tantangan untuk melindungi data dan infrastruktur mereka dari ancaman seperti akses tidak sah, malware, dan aktivitas mencurigakan lainnya yang dapat mengganggu operasional.

Salah satu solusi yang dapat diandalkan untuk menghadapi tantangan ini adalah penerapan system manajemen keamanan informasi, khususnya melalui implementasi *Security Information and Event Management* (SIEM). SIEM adalah sebuah teknologi yang dirancang untuk memantau, mengumpulkan, menganalisis, dan memberikan wawasan tentang aktivitas mencuri atau ancaman keamanan di dalam sistem. Sistem ini menjadi bagian penting dalam membangun *Security Operations Center* (SOC) yang andal dan efisien untuk mendeteksi dan merespon insiden keamanan secara real-time.

Pada Project Based Learning (PBL) semester lalu, kami mendapatkan kesempatan untuk merancang dan mengimplementasikan “*Well Architect SIEM Implementation – SOC 6*”, dengan pendekatan dan pengembangan baru melalui “*SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team*”.

Proyek ini bertujuan untuk menyediakan arsitektur SIEM yang efisien, didukung oleh integrasi teknologi terkini dalam lingkungan SOC yang disimulasikan. Melalui simulasi berbasis game, mahasiswa dapat mengalami langsung proses identifikasi ancaman, analisis data log, serta pelaporan insiden yang relevan bagi tim keamanan.

Dengan pendekatan ini, proyek ini tidak hanya menawarkan solusi teknis, tetapi juga membuka peluang bagi pengguna untuk memahami potensi kerentanan dalam infrastruktur mereka. Implementasi ini diharapkan mampu memberikan panduan praktis dalam membangun sistem keamanan yang lebih kuat, terstruktur, dan responsif terhadap berbagai ancaman siber yang terus berkembang.

## Kajian Pustaka

<https://documentation.wazuh.com/current/index.html>  
<https://learning-if.polibatam.ac.id/mod/resource/view.php?id=5636>  
<https://www.bing.com/ck/a?!&&p=fac1e5f1390e38afJmItDhM9MTcwMzYzNTIwMCZpZ3VpZD0xYmQ3Y2RhZS00NGYyLTZiM2ItMDY5MC1kZjE2NDVhNDZhZjQmaW5zaWQ9NTUwMw&ptn=3&ver=2&hsh=3&fclid=1bd7cdae-44f2-6b3b-0690-df1645a46af4&psq=nginx+apa+dan+manfaat+downloadnya&u=a1aHR0cHM6Ly9pbmRlcGVuZGVuc2kuY29tLzlwMjlvMDIvMTUvcGVuZ2VydGhbi1uZ2lueC1kYW4tbWZmFhdC1wZW5nZ3VuYWFubnlhLyM6fjp0ZXh0PVBldmdlcnRyYW4IMjBOZ2lueCUyMGRhbiUyME1hbmZhYXQIMjBQZW5nZ3VuYWFubnlhJTlwMSUyMFBldmdlcnRyYW4IMjBOZ2lueC1wZW5nZ3VuYWFuJTlwTmdpbnglMjAuLi4IMjA0JTlwQ2FyYSUyMGtldmFhZjE2NDVhNDZhZjQmaW5zaWQ9NTUwMw&ntb=1>

## Perancangan

### A. Deskripsi Produk

SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team adalah konsep implementasi sistem SIEM (Security Information and Event Management) yang dikembangkan secara terstruktur untuk membantu tim keamanan khususnya Blue Team dalam memantau, menganalisis, dan melindungi infrastruktur jaringan dari berbagai ancaman siber. Sistem ini mengintegrasikan pengumpulan log dari berbagai sumber, didukung oleh algoritma analitik canggih untuk meningkatkan deteksi ancaman dan respons insiden secara real time. Proyek ini juga menghadirkan simulasi berbasis permainan (game-based simulation) untuk melatih dan menguji kemampuan Blue Team dalam merespons serangan siber secara interaktif dan realistis. Fitur utama termasuk integrasi dengan alat keamanan seperti firewall dan endpoint protection, deteksi anomaly, serta korelasi data untuk mengidentifikasi aktivitas mencurigakan dan potensi pelanggaran keamanan. Manfaat dari SIEM Development and Game-Based SOC Simulation ini mencakup peningkatan kemampuan monitoring jaringan, deteksi dini terhadap ancaman, respons insiden yang lebih cepat dan terstruktur, serta peningkatan kesadaran situasional dan keterampilan pertahanan dunia maya melalui scenario simulasi yang mendidik. Dengan pendekatan ini, organisasi dapat memperkuat postur keamanan siber mereka secara menyeluruh dan efisien.

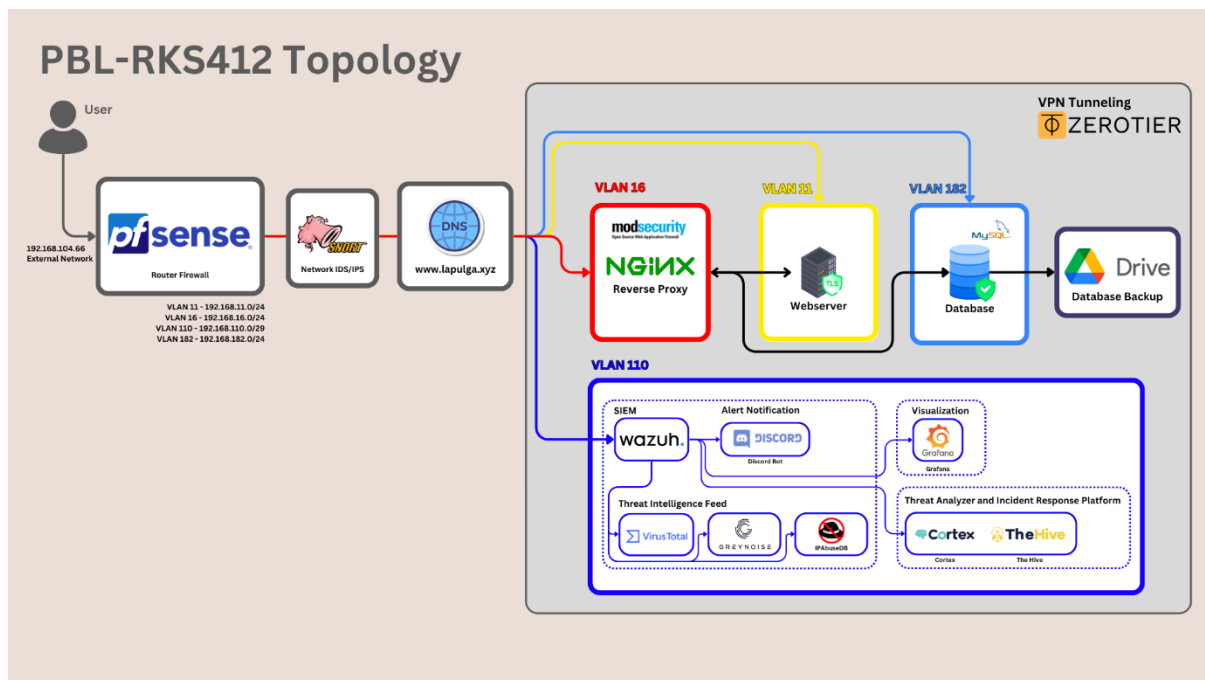
## B. Rancangan Topologi dan Desain

Dalam proyek SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team, sistem dirancang dengan arsitektur logis dan fisik yang terstruktur untuk mendukung pengumpulan log, deteksi ancaman, analisis insiden, serta simulasi pertahanan oleh Blue Team. Rancangan ini bertujuan memberikan visibilitas menyeluruh terhadap aktivitas jaringan, serta membekali mahasiswa dengan pengalaman nyata dalam menerapkan konsep SOC. Integrasi dengan berbagai alat keamanan mendukung simulasi serangan dan pertahanan dalam lingkungan SOC berbasis game. Simulasi ini memungkinkan tim Blue Team melakukan deteksi dini, respon cepat, dan analisis forensik pasca insiden.

Sistem SIEM yang digunakan menjadi pusat pengumpulan dan analisis data log dari berbagai sumber seperti server, endpoint, firewall, dan sistem keamanan lainnya. Dengan teknologi analitik, korelasi log, dan machine learning, sistem dapat mengidentifikasi anomaly atau aktivitas mencurigakan yang dapat memicu respons otomatis maupun manual dari tim Blue Team.

Integrasi SIEM ke dalam lingkungan SOC simulasi ini memberikan pemahaman menyeluruh terhadap pola ancaman siber. Selain meningkatkan efisiensi monitoring dan respons insiden, proyek ini juga memperkuat keterampilan mahasiswa dalam mengelola sistem keamanan yang terstruktur, adaptif, dan responsive terhadap dinamika ancaman yang terus berkembang.

Berikut merupakan topologi yang telah kami buat.



Gambar 1. 1 Rancangan Topologi

Nama	Ip address
VLAN 11 (Web Server)	192.168.11.0/24
VLAN 16 (Proxy)	192.168.16.0/24
VLAN 110 (SIEM)	192.168.110.0/29
VLAN 182 (Database)	192.168.182.0/24
PfSense	192.168.104.66

Dalam infrastruktur yang kami buat terdapat beberapa perangkat dan server berikut adalah rinciannya.

- Firewall (pfSense)

Firewall bertindak sebagai pertahanan pertama untuk jaringan, memonitor semua lalu lintas yang masuk dan keluar. Firewall akan memblokir lalu lintas yang dianggap mencurigakan atau berbahaya untuk melindungi jaringan dari serangan eksternal. Dalam topologi firewall mengatur lalu lintas antara client dan semua server.

- IDS/IPS

IDS/IPS adalah sistem yang digunakan untuk mendeteksi dan mencegah serangan yang terjadi di jaringan. IDS (Intrusion Detection System) untuk memantau lalu lintas jaringan dan memberikan peringatan jika ditemukan aktivitas mencurigakan, sedangkan IPS (Intrusion Prevention System) dapat secara aktif memblokir ancaman tersebut. IDS/IPS seperti snort/suricata diimplementasikan di



dalam jaringan dan terhubung dengan Firewall serta VLAN untuk memperoleh real-time dan memberikan notifikasi jika ada pola serangan, seperti port scanning, brute force, atau exploit yang terdeteksi.

- Web Server

Web server merupakan tempat menyimpan dan menyajikan halaman web serta aplikasi web. Ketika client meminta halaman web tertentu, web server akan mencari dan mengirimkan halaman tersebut. Di web server menggunakan VLAN untuk memisahkan lalu lintas dan meningkatkan keamanan.

- Database

Database adalah tempat menyimpan data yang digunakan oleh aplikasi web. Aplikasi web akan meminta data dari database server Ketika diperlukan dan berfungsi sebagai penyimpanan terpusat untuk data aplikasi, misalnya informasi pengguna, log aktivitas, atau data bisnis lainnya. Di database juga menggunakan VLAN untuk keamanan yang lebih baik. Database juga terkoneksi ke web Server untuk pengembalian data secara langsung.

- SIEM (Wazuh)

Wazuh server adalah alat yang digunakan untuk memantau aktivitas jaringan dan mendeteksi adanya serangan atau ancaman keamanan yang berbasis host (HIDS). Jika Wazuh mendeteksi adanya aktivitas yang mencurigakan, Wazuh akan mengirimkan peringatan. Wazuh juga terhubung ke Firewall untuk mendapatkan akses ke log dari seluruh perangkat dalam jaringan. Di wazuh juga di tempatkan VLAN untuk memiliki visibilitas ke seluruh jaringan

- Proxy Server

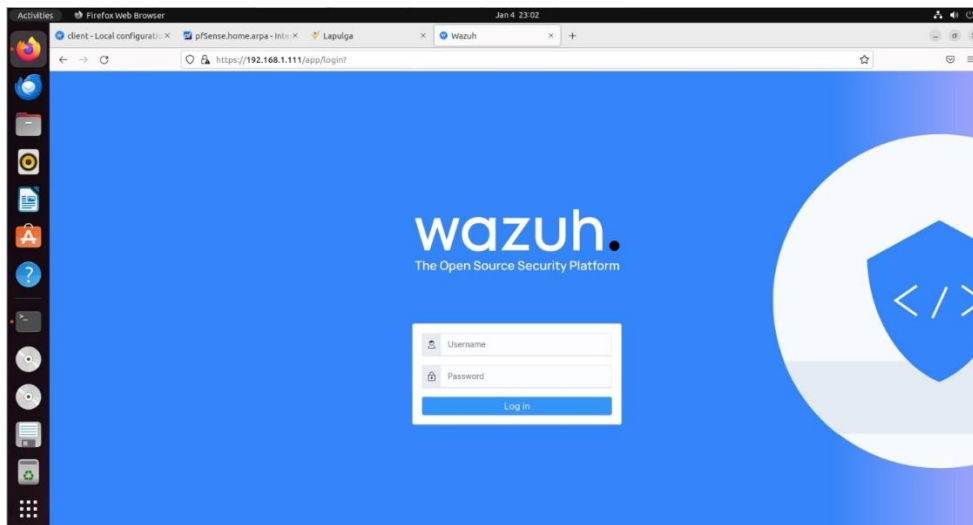
Proxy adalah sebuah server perantara yang bertindak sebagai perantara antara pengguna (client) dan server tujuan di internet. Proxy menerima permintaan dari pengguna, meneruskannya ke server tujuan, lalu mengembalikan respons ke pengguna.

## Implementasi Produk

Pada proyek ini, kami merancang sebuah infrastruktur keamanan jaringan dengan mengimplementasikan konsep SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team. Ini merupakan solusi pemantauan keamanan yang komprehensif, dilengkapi dengan fitur pengumpulan log terpusat, analisis ancaman secara real-time, korelasi data log, dan deteksi anomaly berbasis machine learning. Tujuan utama dari proyek ini adalah menyediakan infrastruktur yang efektif dan efisien dalam mendeteksi dan merespons berbagai ancaman keamanan, mengelola insiden secara sistematis, serta meningkatkan postur keamanan jaringan secara menyeluruh. Rancangan infrastruktur ini mendukung pengambilan keputusan cepat dan tepat oleh tim melalui integrasi dengan berbagai perangkat keamanan seperti firewall, endpoint protection, dan IDS/IPS. Selain itu, proyek ini juga dilengkapi dengan simulasi berbasis game yang memungkinkan mahasiswa berpesan sebagai tim pertahanan dalam merespons scenario serangan siber dan tim attack. Di infrastruktur yang kami rancang, terdapat beberapa perangkat dan server yang terdiri dari:

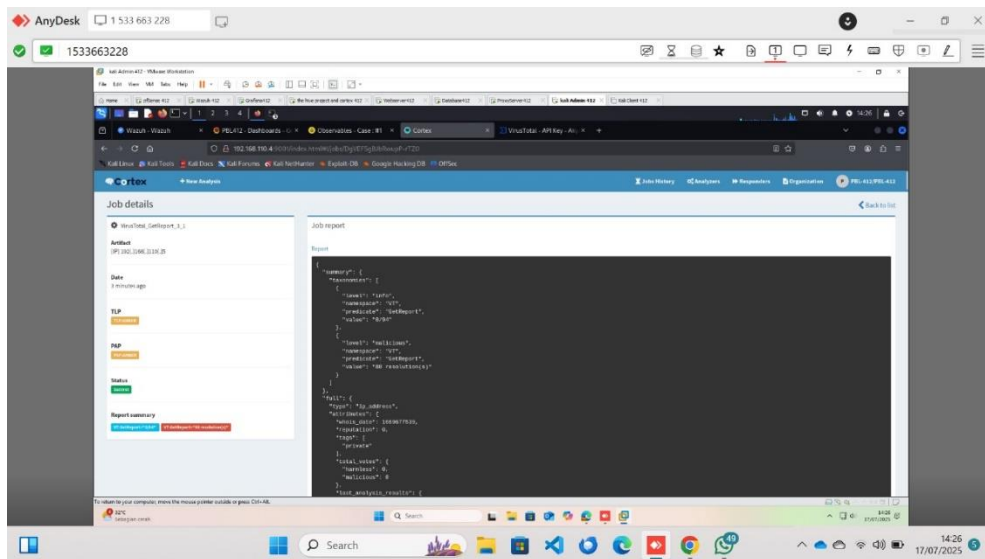
### 1. SIEM

#### 1.1. Wazuh



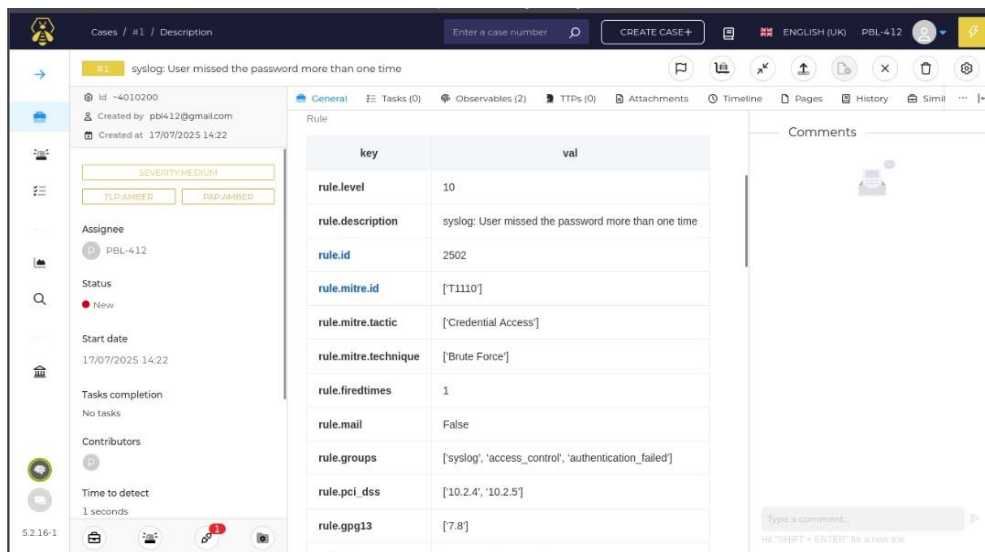
*Gambar 1.2 Wazuh*

#### 1.2. Cortex



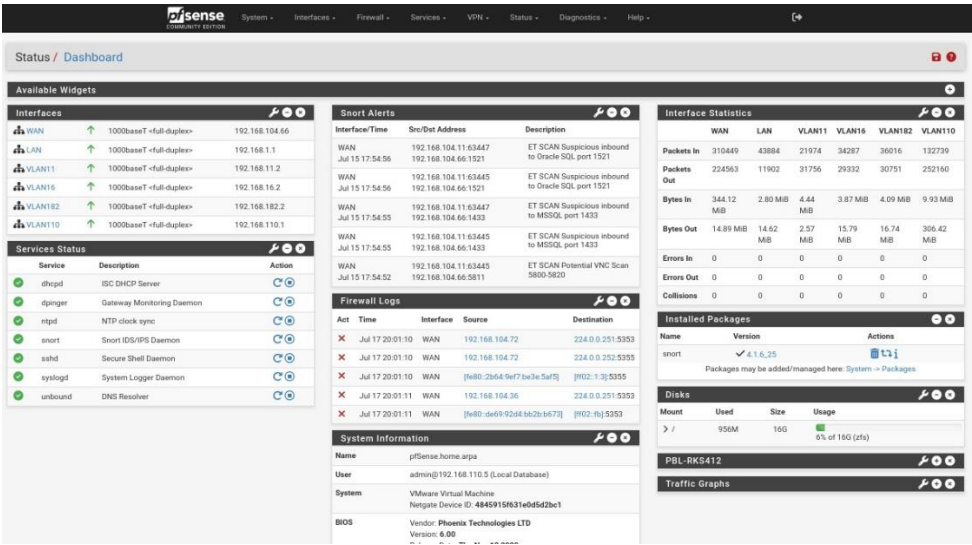
Gambar 1. 3 Cortex

### 1.3. The Hive



Gambar 1. 4 The Hive

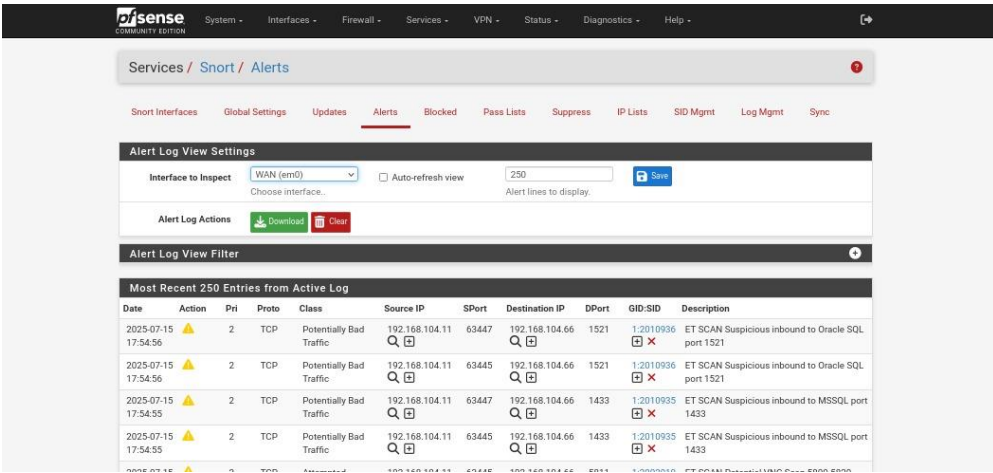
## 2. Firewall



Gambar 1.3 Firewall

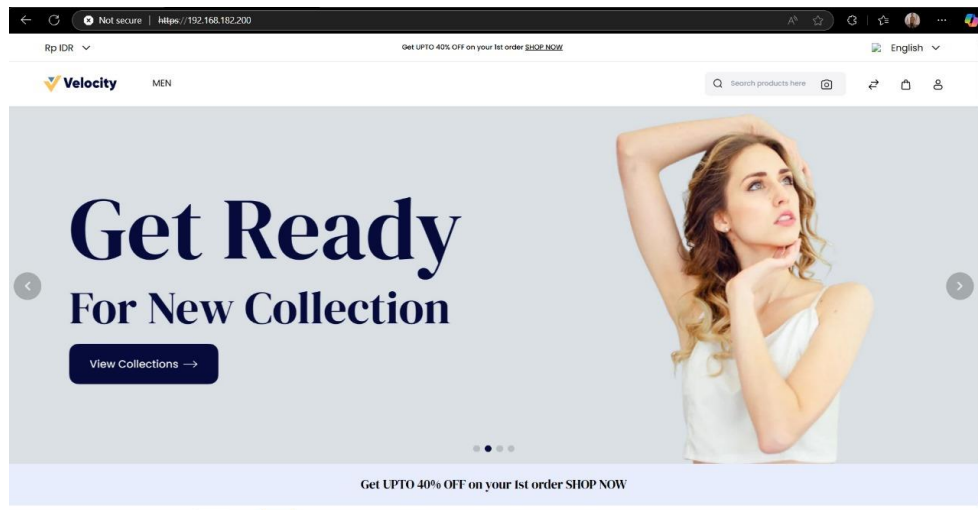
Disini menggunakan jenis Firewall Stateful, ini merupakan platfrom perangkat lunak Firewall dan Router berbasis open-source

3. IDS/IPS



Gambar 1. 6 IDS/IPS

4. Web Server



*Gambar 1. 7 Web Server*

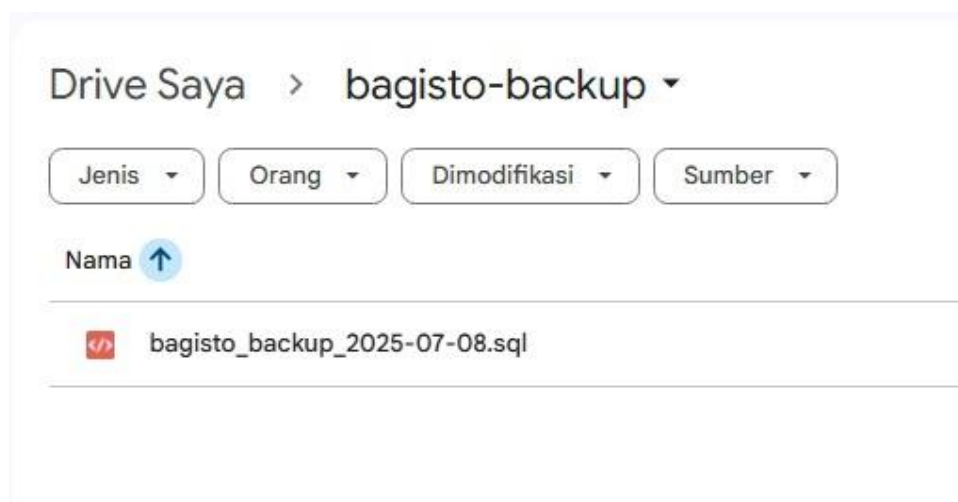
## 5. Database Server

```
mysql> show databases;
+-----+
| Database |
+-----+
| Bagisto  |
| information_schema |
| performance_schema |
+-----+
3 rows in set (0.01 sec)

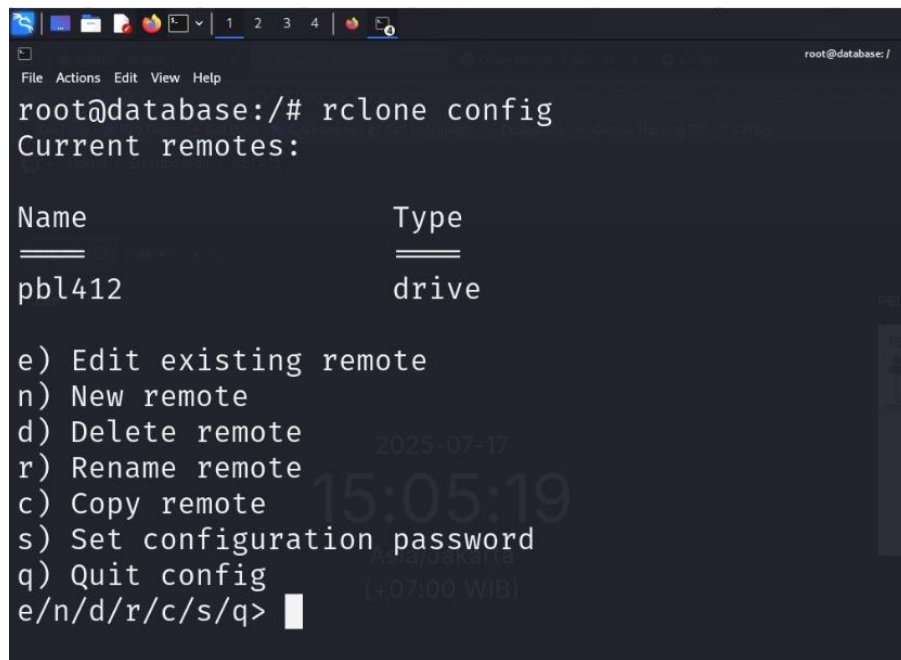
mysql> 
```

*Gambar 1. 8 Database Server*

## 6. Database Backup



*Gambar 1. 9 Database Backup*



```
root@database:/# rclone config
Current remotes:

Name                Type
=====
pbl412              drive

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q>
```

*Gambar 1. 10 Database Backup*

## Future Work

SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team adalah sistem keamanan yang dirancang untuk mengelola pengumpulan log, analisis ancaman, dan deteksi anomali dari berbagai perangkat dalam jaringan. Sistem ini bertujuan untuk memberikan visibilitas dan keamanan yang lebih baik terhadap aktivitas jaringan. Berikut adalah analisis perkembangan dan pengembangan potensial untuk SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team:

### 1. Perbaikan Antarmuka Pengguna (UI/UX)

- Meningkatkan antarmuka pengguna agar lebih mudah dipahami dan digunakan oleh tim keamanan. Visual yang lebih intuitif, navigasi yang lebih jelas, dan pelaporan ancaman yang lebih komprehensif adalah beberapa fokus utama dalam pengembangan ini.

### 2. Kompatibilitas dengan Sistem Beragam

- Memastikan sistem dapat diintegrasikan dengan berbagai perangkat dan platform, termasuk cloud, hybrid, dan on-premise. Hal ini akan meningkatkan fleksibilitas sistem dalam menangani berbagai skenario jaringan.

### 3. Fitur Pemantauan Ancaman Lanjutan

- Menambahkan kemampuan analitik yang lebih canggih, seperti deteksi anomali berbasis machine learning, prediksi ancaman menggunakan AI, dan analisis perilaku pengguna untuk mencegah ancaman sebelum terjadi.

### 4. Aturan dan Kebijakan yang Mudah Dikustomisasi

- Memberikan opsi kepada administrator untuk membuat aturan keamanan dan kebijakan log yang lebih fleksibel sesuai dengan kebutuhan organisasi, termasuk pencocokan aturan dengan standar keamanan terbaru..

### 5. Integrasi dengan Platform Keamanan Lainnya

- Mengembangkan kemampuan integrasi dengan solusi keamanan lain, seperti firewall, endpoint protection, dan threat intelligence untuk memberikan pendekatan keamanan yang holistic.

### 6. Fitur Privasi yang Ditingkatkan

- Memastikan data log dan hasil analisis terjaga keamanannya dengan menerapkan enkripsi end-to-end, akses berbasis peran (RBAC), dan kepatuhan terhadap standar privasi seperti GDPR atau ISO 27001.

### 7. Kolaborasi yang Efektif dalam Tim Keamanan

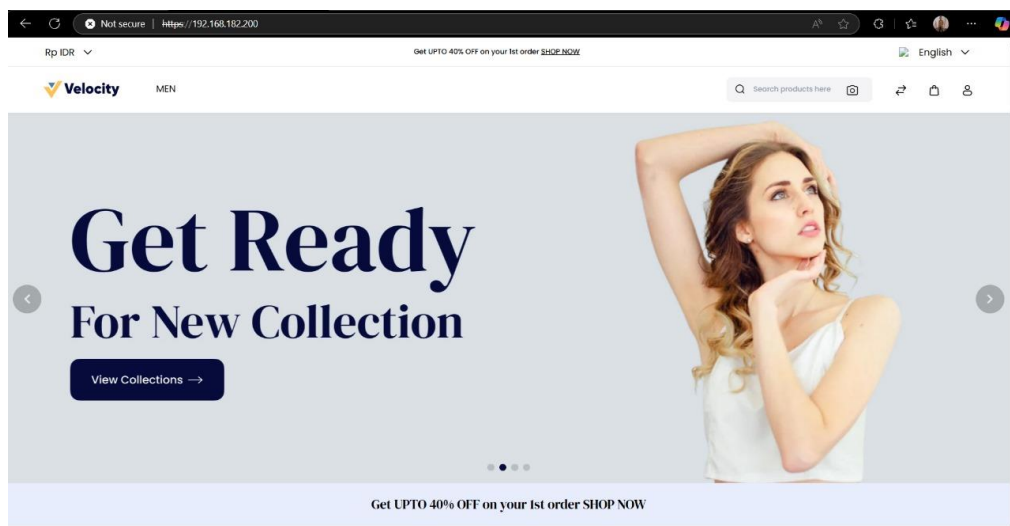
- Mengembangkan fitur untuk mendukung komunikasi dan kolaborasi antar anggota tim keamanan, termasuk integrasi notifikasi real-time, pelacakan insiden bersama, dan dashboard kolaboratif.

Pengembangan ini akan memastikan SIEM Development and Game-Based Security Operation Center (SOC) Simulation Blue Team tetap relevan dengan tantangan keamanan siber yang terus berkembang serta memberikan nilai tambah bagi organisasi yang mengadopsinya.

## Lampiran

Lampiran berisi:

1. [Manual Book](#)
2. Screenshot produk yang telah dibuat beserta link produk.



<https://github.com/sipalinganakdpm/bagisto-306>

3. Screenshot demo/trailer beserta link video.

<https://polibatam.id/VIDEODEMOPBLRKS412>



4. Poster dan video



<https://polibatam.id/PRESENTASIAKHIRPBLRKS412>

5. Dokumen kelengkapan pengajuan HKI beserta link dokumennya.

6. Logbook.

List Logbook Tim - PBL-RKS412

Show 10 entries							
ID	Tahapan	Detail Pengerjaan	Ouput	Mulai	Selesai	Progress	
1	Planning	Melakukan pertemuan dengan manpro membahas terkait timeline pengerjaan proyek, perombakan topologi dan penyelesaian RPP	RPP	2025-03-03	2023-03-14	7%	
2	Planning	Membuat skenario simulasi SOC berbasis game dan menetapkan peran dan tugas blue team dan red team dalam latihan	Skenario SOC dan peran tim	2024-03-24	2025-03-21	12%	
3	Analysis	Melakukan analisis untuk menentukan komponen SIEM seperti agent, server, dashboard, lalu disusun pengumpulan log	Log dan integrasi	2025-03-24	2025-04-04	17%	
4	Analysis	Melakukan analisis terhadap kebutuhan fungsional dan non-fungsional dari sistem dan melakukan scan vulnerability untuk mengidentifikasi kelemahan atau celah keamanan dalam sistem, aplikasi, jaringan	Dokumen analisis	2025-04-07	2025-04-25	23%	
5	Design	Merangkum seluruh aktivitas proyek, menyiapkan laporan dan media untuk presentasi perkembangan paruh semester	Implementasi presentasi	2025-04-28	2025-05-02	30%	
6	Implementasi	Menerapkan VLAN pada infrastruktur proyek dan melakukan reconnaissance serta vulnerability scanning	Hasil scanning dan konfigurasi VLAN awal	2025-05-05	2025-05-09	45%	

7	Implementasi	Mengatur firewall rules pada masing-masing VLAN sesuai kebutuhan infrastruktur dan memastikan setiap segmen jaringan memiliki kontrol akses yang tepat	Konfigurasi firewall per segment VLAN	2025-05-12	2025-05-23	53%
8	Implementasi	Mengimplementasikan IDS/IPS berbasis jaringan pada infrastruktur proyek, menghubungkan ke Wazuh	IDS/IPS terpasang, integrasi awal ke Wazuh	2025-05-26	2025-06-06	62%
9	Implementasi	Melakukan pengujian terhadap IDS/IPS dengan simulasi serangan seperti XSS dan SQL Injection, lalu mendokumentasikan hasilnya	Log deteksi serangan IDS/IPS	2025-06-09	2025-06-13	70%
10	Implementasi	Integrasi alert dari IDS/IPS dan Wazuh ke dalam Discord dan visualisasi melalui Grafana	Notifikasi aktif ke Discord dan dashboard Grafana	2025-06-16	2025-06-20	78%
11	Implementasi	Menyusun dan menguji skenario serangan yang kompleks, melibatkan tim keamanan untuk analisis dan respons	Penyusunan skenario serangan, dokumentasi hasil analisis	2025-06-23	2025-06-27	85%
12	Implementasi	Melakukan audit keamanan menyeluruh terhadap seluruh infrastruktur, memastikan semua konfigurasi sesuai standar keamanan	Audit konfigurasi selesai, laporan audit diserahkan	2025-06-30	2025-07-04	92%
13	Implementasi	Melakukan pelatihan tim keamanan tentang ancaman terbaru dan teknik mitigasi serangan	Pelatihan selesai, materi pelatihan didistribusikan	2025-07-07	2025-07-11	98%
14	Implementasi	Melakukan pemantauan aktif terhadap log sistem dan ancaman, memastikan semua aktivitas tercatat dan dianalisis	Pemantauan aktif dimulai, laporan harian dihasilkan	2025-07-14	2025-07-18	100%