r

**PROGRAM STUDI REKAYASA KEAMANAN SIBER  
JURUSAN TEKNIK INFORMATIKA  
POLITEKNIK NEGERI BATAM  
202X**

**LAPORAN AKHIR**

**PROJECT BASED LEARNING   
“JUDUL”**

# Identitas Proyek

Judul Proyek : Well Architect SIEM Implementation SOC-5

Pengusul Proyek : Hamdani Arif

Manager Proyek : Meidel Fani

Co-Manajer Proyek : -

Klien : Politeknik Negeri Batam

Luaran : 1. Laporan Akhir

2. Video Presentasi dan Demo

3. Poster

4. HKI

|  |  |
| --- | --- |
|  | Laporan akhir |
|  | Poster dan Video |
|  | Dokumen: Rancangan / Desain dan Implementasi sistem (RDI) |
|  | HKI (opsional) |
|  | Proposal lomba (opsional) seperti HelloFest, KMIPN, PKM, dll. |

Tim PBL:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Nama | Nim | Prodi | Pembagian Tugas |
| 1. | Jesicha Simanjuntak | 4332211024 | Rekayasa Keamanan Siber | * KonfigurasiDNS * Topologi * PPT * Laporan * Wazuh |
| 2. | Dina Thesalonika (Team Leader) | 4332211032 | Rekayasa Keamanan Siber | * Webserver * Website * Database * Laporan * HKI |

**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 3 ini yang berjudul “Well Architect SIEM Implementation SOC-5" 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 jga dari berbagai pihak. Dalam kesempatan inni kami ingin berterimakasih kepada :

1. Ibu Meidel Fani selaku manager Project Based Learning
2. Bapak Hamdani Arif selaku wali dosen RKS 3B Malam
3. Seluruh dosen Program Studi Rekayasa Keamanan Siber Politeknik Negeri Batam terimakasih atas kerjasama da abntuannya dalam memberikan bimbingan dan arahannya.
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

[Identitas Proyek 1](#_Toc2041697683)

[Daftar Isi 2](#_Toc1144589812)

[Daftar Gambar 2](#_Toc846524391)

[Daftar Tabel 2](#_Toc1980749543)

[Daftar Lampiran 2](#_Toc1344317188)

[Latar Belakang 2](#_Toc667442246)

[Kajian Pustaka 2](#_Toc637966104)

[Perancangan 2](#_Toc1253574414)

[A. Deskripsi Produk 2](#_Toc613818167)

[B. Rancangan Topologi dan Desain 2](#_Toc1363339512)

[Implementasi Produk 2](#_Toc278389946)

[Future Work 2](#_Toc1497169755)

[Kesimpulan 2](#_Toc750082982)

[Lampiran 2](#_Toc265751680)

# Daftar Gambar

Topologi Jaringan ..............................................................................................1

SIEM(Wazuh).....................................................................................................2

Firewall...............................................................................................................3

Nat......................................................................................................................4

Switch.................................................................................................................5

Database.............................................................................................................6

Webserver..........................................................................................................7

DNS...................................................................................................................8

Website..............................................................................................................9

# Daftar Lampiran

**Lamp 1. Demo Project**

**Lamp 2. Poster**

**Lamp 3. Logbook**

# Latar Belakang

Di zaman sekarang yang di mana teknologi serba canggih Internet kini sudah menjadi kebutuhan yang sangat diperlukan dalam berbagai aspek, salah satunya adalah pendidikan. Internet

Problem Based Learning (PBL) merupakan metode pembelajaran yang dapat mendorong mahasiswa untuk mengenal cara untuk belajar dan bekerja dalam suatu kelompok untuk mencari penyelesaian dari masalah-masalah yang ada di dunia nyata. Teknologi yang semakin maju pastinya diikuti juga dengan ancaman keamanan. Sangat penting ketika kita memiliki sebuah website harus dijaga diikuti dengan memiliki keamanan yang baik. Website dengan sistem keamanan yang buruk biasanya akan menjadi sasaran bagi para hacker untuk melakukan aksi kejahatan. Pada PBL kali ini tim mendapatkan kesempatan untuk melakukan pengujian keamanan atau sering disebut Penetration Testing dimana penilai meniru serangan dunia nyata terhadap beberapa website Politeknik Negeri Batam. Kegiatan ini dilakukan bertujuan untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem, mengetahui dampak yang diakibatkan dari hasil eksploitasi yang dilakukan oleh penyerang pada website Polibatam menggunaakan metode National Institute of Standards and Technology (NIST SP 800-115).

NIST SP 800-115 yang merupakan panduan teknis untuk pengujian dan penilaian keamanan informasi, metodologi yang dikhususkan untuk membantu organisasi dalam melakukan perencanaan tes keamanan informasi. NIST SP 800-115 dengan empat tahapan.

1. Planning

Pada fase ini bertujuan unutuk menentukan beberapa hardware dan software yang digunakan dalam penelitian.

1. Discovery

Pada tahap Discovery terdapat dua fase yang harus dilakukan yaitu: a. Information Gathering b. Vulnerability Scanning

1. Attack

Tahap penyerangan menggunakan Burp Suite dengan tiga teknik penyerangan.

1. Reporting

Tahap penelitian menganalisis hasil serangan. Pada tahap pelaporan, selain menganalisis hasil, juga memberikan kendali atas rekomendasi untuk membuat website lebih aman.

Berdasarkan uraian diatas setelah pengujian selesai dilakukan, pada akhir laporan ini telah dijabarkan hasil celah yang didapat serta tingkat kerentanan yang perlu untuk segera diperbaiki sehingga dapat membantu untuk memperbaiki kegagalan dalam mempertahankan keamanan pada website taxcenter, myinternship, dan talenthub.

# 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=fac1e5f1390e38afJmltdHM9MTcwMzYzNTIwMCZpZ3VpZD0xYmQ3Y2RhZS00NGYyLTZiM2ItMDY5MC1kZjE2NDVhNDZhZjQmaW5zaWQ9NTUwMw&ptn=3&ver=2&hsh=3&fclid=1bd7cdae-44f2-6b3b-0690-df1645a46af4&psq=nginx+apa+dan+manfaat+downloadnya&u=a1aHR0cHM6Ly9pbmRlcGVuZGVuc2kuY29tLzIwMjIvMDIvMTEvcGVuZ2VydGlhbi1uZ2lueC1kYW4tbWFuZmFhdC1wZW5nZ3VuYWFubnlhLyM6fjp0ZXh0PVBlbmdlcnRpYW4lMjBOZ2lueCUyMGRhbiUyME1hbmZhYXQlMjBQZW5nZ3VuYWFubnlhJTIwMSUyMFBlbmdlcnRpYW4lMjBOZ2lueCxwZW5nZ3VuYWFuJTIwTmdpbnglMjAuLi4lMjA0JTIwQ2FyYSUyMGtlcmphJTIwTmdpbnglMjA&ntb=1>

# Perancangan

## Well Architect SIEM Implementation

Istilah "Well-Architected SIEM Implementation" mengacu pada desain dan implementasi sistem Security Information and Event Management (SIEM) mengikuti praktik dan pedoman terbaik. Proses ini biasanya melibatkan langkah-langkah seperti perencanaan, instalasi, konfigurasi, fine-tuning, dan manajemen dan pemeliharaan berkelanjutan AWS Well-Architected Framework memberikan panduan untuk membangun aplikasi cloud yang aman dan efisien, termasuk keamanan, keunggulan operasional, keandalan, performa.

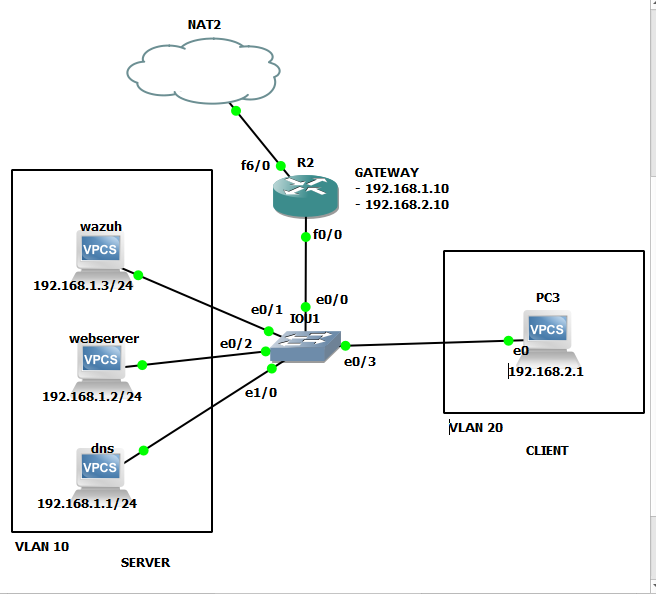
Implementasi SIEM (Security Information and Event Management) merupakan upaya yang komprehensif dan harus mencakup berbagai aspek dalam rangkaian proses keamanan informasi perusahaan.Merancang dan mengimplementasikan pengumpulan data dari berbagai sumber, seperti server, jaringan, aplikasi, dan perangkat endpoint.Memonitor dan menganalisis data log dan aktivitas secara real-time untuk mengidentifikasi ancaman dan insiden keamanan.Memastikan bahwa implementasi SIEM sesuai dengan regulasi dan kebijakan perusahaan serta peraturan yang berlaku di industri Anda.Melatih tim keamanan dan pengguna lainnya dalam menggunakan antarmuka SIEM dan memahami laporan serta peringatan yang dihasilkan.Memastikan bahwa solusi SIEM dapat dengan mudah berkembang sesuai dengan pertumbuhan perusahaan dan kebutuhan yang lebih tinggi.Penting untuk dicatat bahwa implementasi SIEM adalah proses berkelanjutan dan melibatkan kerjasama tim keamanan informasi, profesional TI, dan manajemen perusahaan.

## Rancangan Topologi dan Desain

Sistem SIEM harus dirancang dengan arsitektur logis dan fisik yang mendefinisikan komponen, persyaratan infrastruktur, dan model penyebaran.Misalnya, sistem dapat dirancang untuk menyertakan server SIEM terpusat yang mengumpulkan dan menganalisis data log dari berbagai sumber.Sistem SIEM harus dirancang untuk menangani volume data yang dihasilkan oleh infrastruktur TI organisasi. Sistem harus terukur untuk mengakomodasi pertumbuhan dan ekspansi di masa depan.

GNS3 (Graphical Network Simulator 3) adalah merancang, mengonfigurasi, dan mensimulasikan jaringan secara virtual. Alat ini digunakan terutama untuk pembelajaran, pengembangan, dan pengujian konsep jaringan, konfigurasi perangkat jaringan, dan interaksi antara perangkat-perangkat tersebut, GNS3 digunakan oleh siswa, mahasiswa, dan profesional TI untuk memahami konsep jaringan, protokol, dan teknologi. GNS3 digunakan untuk menguji skenario dan pemecahan masalah dalam jaringan tanpa mengganggu produksi nyata,memungkinkan insinyur jaringan untuk merancang dan menguji prototipe jaringan sebelum diterapkan dalam lingkungan produksi.GNS3 mendukung emulasi berbagai perangkat jaringan, termasuk router, switch, firewall, dan bahkan server.

Berikut merupakan topologi yang telah kami buat.



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

Router

Router merupakan perangkat keras jaringan yang dapat mengelola lalu lintas antar jaringan dengan meneruskan paket data ke alamat ip yang dituju dengan memetakan jalur route terlbeih dahulu.

Switch

Switch adalah perangkat keras jaringan yang berfungsi untuk menghubungkan beberapa perangkat komputer dalam suatu jaringan. proses ini memungkinkan pengguna bertukar data dan informasi ke perangkat yang dituju.

SIEM(Wazuh)

SIEM, singkatan dari Security Information and Event Management, adalah teknologi yang kuat yang menggabungkan manajemen informasi keamanan (SIM) dan manajemen peristiwa keselamatan (SEM) fungsi. Pada projek kali ini kami menggunakan Wazuh sebagai SIEM pada infrastruktur kami. Wazuh adalah platform keamanan yang dirancang untuk mendeteksi ancaman keamanan dan memantau aktivitas keamanan pada suatu sistem. Ini merupakan perangkat lunak sumber terbuka yang menyediakan solusi keamanan informasi untuk organisasi. Wazuh mencakup fungsi deteksi ancaman, manajemen log, dan keamanan informasi.

Monitoring Desktop

Kami menggunakan VirtulaBox sebagai monitoring desktop.

Database

Database adalah kumpulan data yang terstruktur dan disimpan secara sistematis di komputer atau sistem komputer. Data dalam database dapat diakses, dikelola, dan diperbarui dengan mudah menggunakan perangkat lunak database tertentu. Database bertujuan untuk menyimpan dan mengorganisir informasi sehingga dapat dengan efisien diambil atau dimanipulasi.

Webserver

Web server adalah perangkat keras atau perangkat lunak yang menyediakan layanan untuk mengakses halaman web atau konten lainnya melalui internet. Web server bertanggung jawab untuk menerima permintaan HTTP (Hypertext Transfer Protocol) dari klien, seperti browser web, dan mengirimkan respons yang berisi halaman web atau sumber daya lain yang diminta. Disini kami menggunakan Nginx sebagai webserver kami, NGINX adalah web server yang juga berfungsi sebagai email proxy, reverse proxy, dan load balancer. Struktur software ini bersifat asinkron dan event-driven; yang memungkinkan banyak request atau permintaan diproses pada waktu bersamaan.

DNS Server

DNS adalah singkatan dari Domain Name System, sebuah sistem yang akan memudahkanmu saat hendak mengunjungi sebuah situs web. Jika tidak menggunakan DNS, kamu harus menulis alamat IP (IP Address) seperti 172.18.11.123 untuk mengakses suatu website. Jadi fungsi utama dari DNS Server adalah menghubungkan URL dengan IP Address agar pengguna lebih mudah untuk mengakses suatu situs di internet

# Implementasi Produk

Pada Projek ini kami merancang sebuah infrastruktur yang baik dengan mengimplementasikan SIEM didalamnya, disini kami menggunakan Wazuh sebagai SIEM. Alasan kami memilih wazuh adalah karena Wazuh adalah platform yang open source serta mendukung berbagai platform seperti windows, linux dan macOS. Di infrastruktur yang kami rancang, terdapat beberapa perangkat dan beberapa server yang terdiri dari.

1) SIEM(Wazuh)

2) Router

3) Switch

4) Database Server

5) WebServer

6) DNS Server

# Future Work

SIEM itu sangatlah luas, bukan hanya sekedar monitoring terhadap layanan kita. Untuk kedepannya kami ingin merancang SIEM yang terintegrasi dengan teknologi terbaru, serta mengembangkan fungsi otomatisasi untuk menanggapi ancaman yang terdeksi, sehingga dapat membantu mengurangi waktu response terhadap serangan dan pemulihan yang cepat

Kesimpulan Implementasi SIEM (Security Information and Event Management) yang baik, atau yang dikenal sebagai "well-architected SIEM implementation," mencakup sejumlah prinsip dan praktik terbaik untuk memastikan efektivitas dan keberhasilan solusi keamanan informasi dan manajemen kejadian. Berikut adalah kesimpulan terkait topik ini:

1. Arsitektur yang Baik - SIEM harus dirancang dengan arsitektur yang baik, mempertimbangkan kebutuhan organisasi dan kompleksitas infrastruktur IT. - Integrasi yang baik dengan perangkat keras dan perangkat lunak lainnya perlu diperhatikan agar SIEM dapat mengumpulkan dan menganalisis data dari berbagai sumber.

2. Pengumpulan dan Normalisasi Data - Pengumpulan data yang efektif dari berbagai sumber, termasuk log perangkat jaringan, server, aplikasi, dan perangkat endpoint. - Normalisasi data untuk memastikan konsistensi dan kemudahan analisis.

3. Ketepatan dan Relevansi - Fokus pada pengumpulan data yang relevan dengan keamanan dan kejadian yang signifikan bagi organisasi. - Pengaturan aturan dan filter yang tepat untuk mengurangi kebisingan dan memprioritaskan kejadian yang lebih penting.

4. Deteksi dan Respon Cepat - Implementasi aturan deteksi yang cerdas dan analisis perilaku untuk mendeteksi ancaman keamanan dengan cepat. - Respon cepat terhadap insiden, termasuk otomatisasi untuk tindakan respons yang lebih cepat.

5. Kepatuhan dan Audit - Memastikan kepatuhan dengan regulasi keamanan dan audit internal. - Pemantauan dan pelaporan secara teratur untuk mendukung proses audit dan pelaporan keamanan.

6. Skalabilitas dan Kinerja - Arsitektur yang dapat diskalakan untuk menangani pertumbuhan data dan kebutuhan keamanan yang berkembang. - Pemantauan kinerja untuk memastikan SIEM tetap efisien dan responsif.

7. Pelatihan dan Kesadaran - Pelatihan yang adekuat bagi personel untuk menggunakan dan mengelola SIEM dengan efektif. - Peningkatan kesadaran keamanan di seluruh organisasi untuk mendukung pemahaman tentang kebijakan dan prosedur keamanan.

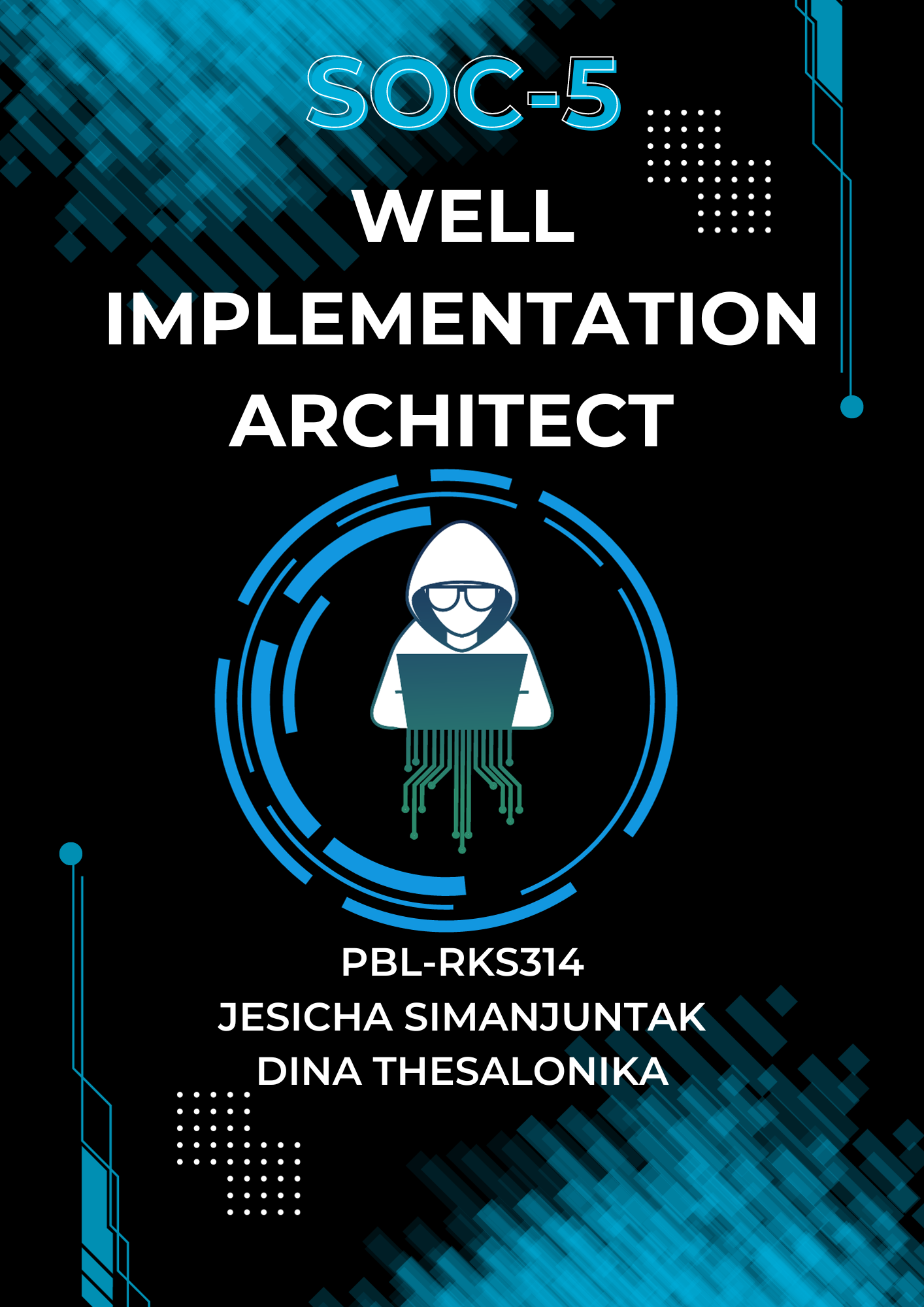
8. Integrasi dengan Keamanan Lainnya - Integrasi SIEM dengan alat keamanan lainnya seperti IDS/IPS, antivirus, dan solusi keamanan lainnya untuk menyediakan visibilitas yang komprehensif. - Kolaborasi dengan sistem SIEM lainnya jika diperlukan untuk keamanan yang lebih luas.

Implementasi SIEM yang baik menggabungkan teknologi, proses, dan orang untuk membentuk pendekatan holistik terhadap keamanan informasi, memungkinkan organisasi untuk mendeteksi, merespons, dan mencegah ancaman keamanan dengan lebih efektif

# Lampiran

Lampiran berisi:

1. Manual book
2. Screenshot produk yang telah dibuat beserta link produk.
3. Screenshot demo/trailer beserta link video.
4. Poster dan video



1. Dokumen kelengkapan pengajuan HKI beserta link dokumennya.
2. Logbook.
3. Proposal lomba (jika ada).