Nomor ID	**:**	*PBL-RKS321*
Pengusul Proyek	**:**	*Maidel Fani, S.Pd., M.Kom.*
Manajer proyek	**:**	*Muhammad Idris, S.Tr., M.Tr.Kom*
Judul Proyek	**:**	*Pengembangan Well-Architect Infrastruktur SIEM dengan agregasi sistem CTI*
Luaran	**:**	*SIEM Architecture, Laporan Akhir, Poster, Video Demo*
Sponsor	**:**	-
Biaya	**:**	*RP 0,-*
Klien/Pelanggan	**:**	*Maidel Fani, S.Pd., M.Kom.*
Waktu	**:**	*1 Semester (14 minggu)*

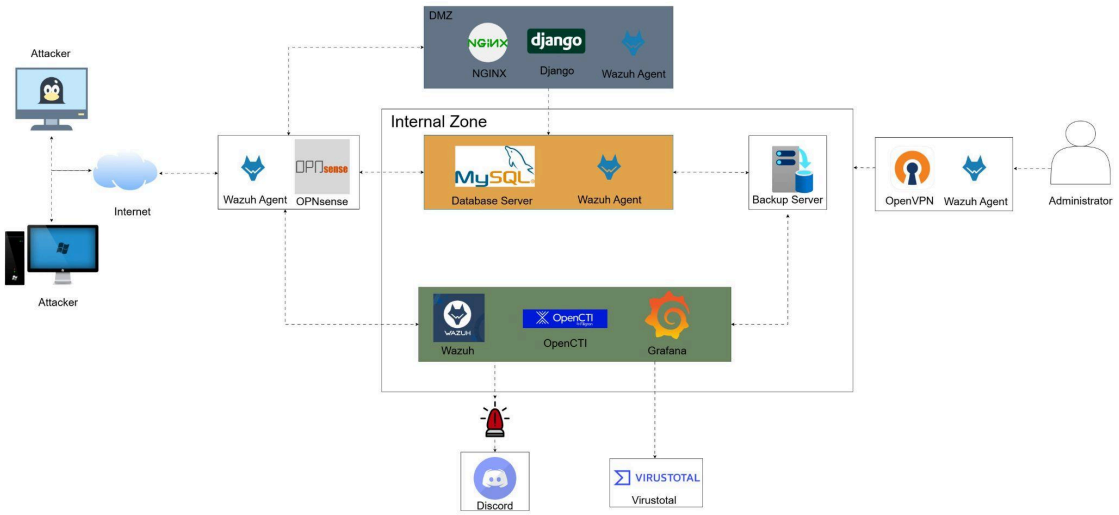
1. Ruang lingkup

Pada semester 3 ini, mahasiswa melaksanakan proyek berbasis Project Based Learning (PBL) dengan tema Well-Architect dan SIEM. PBL ini dirancang untuk memberikan pengalaman langsung dalam memahami konsep perancangan infrastruktur, pengelolaan layanan, serta penerapan sistem monitoring keamanan. Dengan pendekatan ini, mahasiswa tidak hanya belajar teori, tetapi juga mampu mempraktikkannya melalui pembangunan sistem yang lebih nyata.

Ruang lingkup proyek mencakup beberapa aspek utama. Pertama, pengembangan arsitektur infrastruktur yang memperhatikan aspek keamanan, ketersediaan, dan keandalan sistem. Kedua, pengembangan layanan web sederhana yang digunakan sebagai media uji coba (test bed) dalam simulasi keamanan. Ketiga, pengelolaan basis data yang mendukung operasional sistem, termasuk penerapan mekanisme cadangan data untuk menjaga kontinuitas layanan. Selain itu, proyek juga mencakup penerapan sistem monitoring keamanan yang terintegrasi dengan Security Information and Event Management (SIEM) dan Cyber Threat Intelligence (CTI), sehingga mahasiswa dapat belajar menganalisis ancaman serta memahami proses deteksi insiden keamanan secara menyeluruh. Penerapan administrasi sistem dan jaringan turut menjadi bagian penting, seperti pengaturan server, pengelolaan akses, hingga konfigurasi keamanan dasar untuk menjaga stabilitas dan integritas layanan.

Melalui pelaksanaan PBL ini, mahasiswa diharapkan mampu mengembangkan keterampilan teknis, berpikir kritis, serta memahami alur kerja yang mendukung terbentuknya sebuah Security Operation Center (SOC). Dengan demikian, proyek ini tidak hanya berfungsi sebagai sarana pembelajaran, tetapi juga sebagai bekal untuk menghadapi tantangan di bidang keamanan siber pada tahap berikutnya

2. Desain Umum



Desain umum sistem ini dirancang untuk membangun arsitektur Well-Architected SIEM (Security Information and Event Management) dengan prinsip defense in depth. Topologi dibagi menjadi beberapa zona yang tersegmentasi untuk memisahkan fungsi layanan dan meningkatkan keamanan.

1. **Lapisan Keamanan Utama (Firewall & Routing)**
   OPNsense ditempatkan sebagai gerbang utama antara Internet, DMZ, dan Internal Zone. Komponen ini berfungsi ganda sebagai router sekaligus firewall dengan dukungan IDS/IPS untuk mendeteksi serta mencegah serangan dari luar. Dengan segmentasi ini, lalu lintas jaringan dapat difilter sehingga hanya koneksi yang sah yang bisa melewati tiap zona.
2. **Zona DMZ (Demilitarised Zone)**
   DMZ menampung layanan publik yang berinteraksi langsung dengan pengguna luar. Di dalamnya terdapat Nginx + Django sebagai aplikasi web utama serta Wazuh Agent yang bertugas mengirimkan log aktivitas ke sistem SIEM di Internal Zone. Penempatan di DMZ memastikan jika aplikasi publik mengalami kompromi, dampaknya tidak langsung menyentuh aset kritis.
3. **Zona Internal**
   Internal Zone menyimpan aset penting dan sistem inti. Komponen di dalamnya meliputi:
   - MySQL Database sebagai pusat penyimpanan data yang hanya dapat diakses melalui aplikasi di DMZ dengan aturan firewall yang ketat.
   - Backup Server untuk menjaga ketersediaan dan pemulihan data jika terjadi kegagalan atau insiden.
   - Komponen SIEM (Wazuh, OpenCTI, Grafana) yang berfungsi untuk mengumpulkan log, menganalisis ancaman, serta menampilkan informasi dalam bentuk dashboard visual.
4. **Integrasi Eksternal & Alerting**
   Sistem SIEM dirancang untuk menghasilkan alert secara real-time. Setiap deteksi ancaman dari Wazuh akan dikirim ke VirusTotal untuk validasi tambahan, lalu diteruskan ke Discord sebagai media notifikasi agar tim SOC dapat merespons secara cepat dan efisien.
5. **Akses Administrator**
   Administrator hanya dapat mengakses sistem melalui OpenVPN, sehingga jalur manajemen bersifat aman dan tidak terbuka langsung ke Internet. Hal ini memastikan kontrol penuh terhadap sistem sekaligus meminimalisir risiko intrusi.

Dengan desain ini, arsitektur SIEM mampu menyediakan keamanan berlapis melalui segmentasi zona, kontrol akses yang ketat, analisis ancaman berbasis CTI, hingga mekanisme notifikasi instan. Pendekatan ini tidak hanya memperkuat sistem dari sisi teknis, tetapi juga mendukung praktik terbaik dalam manajemen keamanan jaringan.

3. Konstruksi Produk

1. **Penelitian Konsep dan Dasar**
   Tahap awal dimulai dengan menyusun kerangka konseptual untuk membangun sistem keamanan berbasis Well-Architected SIEM. Prinsip utama yang diterapkan adalah defense in depth, yaitu dengan membuat segmentasi jaringan yang tegas antara Demilitarized Zone (DMZ) dan Internal Zone.

   Pada desain ini, OPNsense dipilih sebagai komponen sentral yang memiliki peran ganda. Selain berfungsi sebagai router, OPNsense juga bertugas sebagai firewall yang mengatur lalu lintas antar zona, menjaga keamanan komunikasi, serta mendukung fitur IDS/IPS untuk mendeteksi dan mencegah intrusi.Untuk memperkuat landasan, dilakukan kajian literatur mengenai konsep SIEM, Cyber Threat Intelligence (CTI), manajemen jaringan, dan praktik terbaik keamanan siber. Dari hasil penelitian, ditetapkan komponen inti sistem, yaitu:
   - Nginx web server dan Django python pada zona DMZ sebagai aplikasi web.
   - MySQL Database pada Internal Zone sebagai pusat penyimpanan data.
   - Wazuh, OpenCTI, dan Grafana sebagai inti SIEM yang bertugas mengelola log, mengkorelasikan ancaman, serta menyajikan visualisasi.

   Selain itu, teknologi pendukung juga dipilih untuk memperkuat keamanan dan efisiensi sistem. OpenVPN digunakan sebagai jalur akses administrator, VirusTotal diintegrasikan sebagai layanan eksternal untuk validasi ancaman, dan Discord dimanfaatkan sebagai kanal komunikasi real-time untuk tim SOC.

2. **Perancangan Sistem**
   Perancangan dilakukan dengan menggambarkan alur komunikasi antar komponen sekaligus membagi peran setiap zona jaringan.
   - **Zona DMZ**
     Zona ini menampung layanan publik, yaitu aplikasi web berbasis Nginx + Django, serta Wazuh Agent yang bertugas mengumpulkan aktivitas sistem dan mengirimkan log ke Internal Zone untuk dianalisis lebih lanjut.
   - **Zona Internal**
     Zona ini menyimpan aset paling vital, di antaranya:
     - MySQL Database, yang hanya dapat diakses aplikasi dari DMZ melalui aturan ketat firewall.
     - Backup Server untuk menjamin ketersediaan dan kontinuitas data. Wazuh sebagai pusat pengelolaan log.
     - Dan OpenCTI untuk korelasi data ancaman, serta Grafana sebagai media visualisasi yang menyajikan informasi keamanan secara interaktif.
   - **Integrasi Alerting**
     Mekanisme alert dirancang agar setiap peringatan dari Wazuh dapat diteruskan ke VirusTotal untuk divalidasi. Setelah itu, hasil alert akan dikirim secara otomatis ke Discord, sehingga tim SOC dapat segera mengambil tindakan.
   - **Akses Administrator**
     Seluruh akses administrator hanya diizinkan melalui OpenVPN, sehingga jalur manajemen sistem tetap aman dan terhindar dari akses langsung melalui Internet.

   Dengan rancangan ini, OPNsense diposisikan sebagai pondasi utama yang mengontrol, memisahkan, dan mengamankan arus komunikasi antar zona jaringan.

3. **Implementasi dan Integrasi**
   Tahap implementasi dilakukan dengan merealisasikan desain menjadi sistem yang berjalan nyata. OPNsense dikonfigurasi sebagai firewall sekaligus penghubung antara Internet, DMZ, dan Internal Zone,

serta diaktifkan fungsi IDS/IPS untuk deteksi dini ancaman. Di sisi DMZ, aplikasi web berbasis Nginx + Django dijalankan, dengan Wazuh Agent yang terus memantau aktivitas server dan mengirimkan log ke internal.
Pada Internal Zone, MySQL Database diinstal dan diatur agar hanya menerima koneksi dari aplikasi di DMZ. Backup Server disiapkan untuk menjamin keberlangsungan data. Sementara itu, komponen utama SIEM dipasang: Wazuh untuk deteksi dan pengelolaan log, OpenCTI sebagai pusat threat intelligence, serta Grafana untuk menyajikan data dalam bentuk visual yang mudah dipahami.

Untuk mendukung mekanisme respons ancaman, integrasi alert dikembangkan agar hasil deteksi dari Wazuh dapat diverifikasi melalui VirusTotal, lalu secara otomatis diteruskan ke Discord sebagai notifikasi real-time untuk tim SOC. Selain itu, OpenVPN dipasang untuk menjamin keamanan akses administrator.

4. Uji Coba dan Evaluasi

Tahap akhir berupa pengujian sistem, yang dilakukan untuk memastikan seluruh komponen berjalan sesuai dengan tujuan perancangan. Beberapa skenario uji meliputi:

- Uji Fungsionalitas → memastikan aplikasi web di DMZ berjalan normal, database dapat diakses sesuai aturan, dan mekanisme backup berjalan dengan baik.
- Uji Keamanan → simulasi serangan dilakukan untuk menilai kemampuan OPNsense dalam memblokir ancaman dan menguji efektivitas deteksi dari Wazuh.
- Uji Integrasi → mengecek aliran log dari DMZ ke Wazuh, proses korelasi ancaman di OpenCTI, hingga penyajian informasi di Grafana.
- Uji Alerting → memverifikasi bahwa peringatan keamanan terkirim ke VirusTotal dan diteruskan secara real-time ke Discord.

4. Kebutuhan Peralatan/Perangkat dan Bahan/Komponen

Fase/Proses	Peralatan/Perangkat (SW/HW)			Bahan/Komponen		
	Nama	Jumlah	Catatan	Nama	Jumlah	Catatan
Penelitian konsep dan dasar	Laptop/ Computer	4	HW			
	Canva	4	SW			
	Google Docs, Draw.io	4	SW			
	Zoom, Discord	4	SW			
Perancangan sistem aplikasi	Laptop/ Computer	4	HW			
	Draw.io	4	SW			
	Cisco Packet Tracer	4	SW			
	Canva	4	SW			
	Zoom, Discord	4	SW			
Implementasi dan integrasi	Laptop/ Computer	4	HW			
	Github	4	SW			
	Virtual Machine	7	SW			
	Visual Code	4	SW			
	Zoom, Discord	4	SW			
Uji coba dan evaluasi	Laptop/ Computer	7	HW			
	GNS3/ Cisco Packet Tracer	2	SW			
	Virtual Machine	7	SW			
	Zoom, Discord	4	SW			

5. Tantangan dan Isu

No	Fase/Proses Peralatan/Bahan	Tantangan/Isu	Level Risiko*	Rencana Tindakan	Catatan
1	Planning & Analysis	- Kurang pemahaman terhadap apa saja yang akan dibutuhkan. Berkoordinasi dengan anggota tim.	H	- Mencari referensi dari berbagai media yang ada dan juga berdiskusi dengan manpro. - Tetap menjaga komunikasi dengan sesama tim supaya tetap aktif.	
2	Design	- Kurang kreatif. - Tidak menarik.	H	- Mencari lebih banyak inspirasi. - Mencari cara supaya lebih kreatif.	
3	Implementation	- Perangkat kurang memadai.	H	- Menggunakan perangkat yang tersedia di Lab.	
4	Testing & Integration	- Kendala saat menjalankan atau mencoba hasil proyek.	H	- Mencari bantuan ataupun solusi terkait kendala yang dialami.	

6. Estimasi Waktu Pekerjaan

Fase/Proses	Uraian Pekerjaan	Estimasi Waktu	Catatan
Penelitian konsep dan dasar	1. Membuat RPP. 2. Riset mengenai produk yang akan dibuat.	3 Minggu	…
Perancangan sistem aplikasi	1. Mendesain Prototipe Produk. 2. Mendesain topologi Produk.	2 Minggu	…
Implementasi dan integrasi	1. Penerapan Monitoring web dan web flask. 2. Penerapan Proxy Linux di Server.	7 Minggu	…
Uji coba dan evaluasi	1. Pengujian sistem secara keseluruhan dan validasi hasil. 2. Penyatuan beberapa elemen atau komponen menjadi satu kesatuan yang utuh.	2 Minggu	…

7. Biaya Proyek (Biaya Bahan dan Peralatan)

Fase/Proses	Uraian Pekerjaan	Perkiraan Biaya	Catatan
	…	…	
	…	…	
	…	…	
…	…	…	
	Total	**Rp 0.00**	

8. Tim proyek (Dosen, Laboran dan/atau Mahasiswa)

No	Nama	NIK/NIM	Program Studi
1	Muhammad Idris, S.Tr., M.Tr.Kom (Manajer Proyek)	122283	**Dosen** Rekayasa Keamanan Siber
2	Maidel Fani, S.Pd., M.Kom.	117192	**Dosen** Rekayasa Keamanan Siber
3	Agus Fatulloh, S.T., M.T	107051	**Dosen** Rekayasa Keamanan Siber

No	Nama	NIK/NIM	Program Studi
4	Antoni Haikal, S.S.T., MT	122276	**Dosen** Rekayasa Keamanan Siber
5	Festy Winda Sari, M.Sc	122288	**Dosen** Rekayasa Keamanan Siber
6	Nelmiawati, B.CS., M.Comp.Sc	115148	**Dosen** Rekayasa Keamanan Siber
7	Nur Zahrati Janah, S.Kom, M.Sc	112087	**Dosen** Teknik Informatika
8	Agus Riady A,Md.Kom	224345	**Laboran** Rekayasa Keamanan Siber
9	Syafiq Adi Kurniawan	4332401013	**Mahasiswa** Rekayasa Keamanan Siber
10	Syahdan Arief S	4332401006	**Mahasiswa** Rekayasa Keamanan Siber
11	Muhammad Reza Pahlevi	4332401020	**Mahasiswa** Rekayasa Keamanan Siber
12	Helena Yolanda Amelia	4332401027	**Mahasiswa** Rekayasa Keamanan Siber

9. Ruang Kerja (Workspace)/Laboratorium/Workshop

Gedung TA 11.3.

10. Mata Kuliah, Capaian Pembelajaran dan Capaian Pembelajaran Mata Kuliah yang terlibat

No.	Nama Mata Kuliah	Capaian Pembelajaran	Capaian Pembelajaran Mata Kuliah
1.	Hukum dan Etika Keamanan Siber	Mahasiswa mampu menjabarkan dan merinci hukum, peraturan perundangan, etika yang terkait teknologi informasi dan keamanan siber serta pelaksanaannya dalam pekerjaan	1. Menjelaskan secara rinci Hukum, peraturan perundangan di Indonesia dan Internasional terkait keamanan siber. 2. Menjelaskan secara rinci Etika dalam dunia siber: Privasi, Akurasi, Properti, Akses. 3. Menjelaskan etika profesi teknologi informasi dan keamanan siber serta aplikasinya dalam profesi 4. Mengklasifikasi tindakan yang termasuk cybercrime 5. Mendeteksi tindakan cybercrime dan mengemukakan referensi hukum yang sesuai terhadap tindakan tersebut
2.	Kriptografi Terapan	Mahasiswa diharapkan mampu dalam mengidentifikasi dan menganalisis teknik kriptografi yang sesuai untuk mengamankan data.	1. Mahasiswa mampu menjelaskan konsep dasar kriptografi dan fungsinya dalam menjaga keamanan pesan. 2. Mahasiswa mampu membandingkan berbagai macam algoritma kriptografi dari berbagai jenis (simetris, asimetris, hash, tanda tangan digital). 3. Mahasiswa mampu menentukan algoritma kriptografi yang sesuai untuk mengamankan pesan, baik yang terkirim maupun tersimpan di dokumen. 4. Mahasiswa mampu membuat program menggunakan kriptografi untuk mengamankan pesan. 5. Mahasiswa mampu menerapkan kriptografi pada protokol jaringan, email, file, VPN, dan sistem modern seperti blockchain. 6. Mahasiswa mampu bekerja sama dalam tim untuk merancang dan mengimplementasikan solusi keamanan berbasis kriptografi dengan sikap profesional dan etis

3.	Administrasi Sistem Komputer	Mahasiswa mampu menjelaskan dan menerapkan segala sesuatu yang dibutuhkan untuk menjadi administrator seperti melakukan instalasi, konfigurasi, proses administrasi dan layanan server yang dibutuhkan.	1. Mahasiswa dapat menjelaskan peran dari administrator sistem. 2. Mahasiswa dapat menjelaskan distribusi dan paket pada sistem server. 3. Mahasiswa dapat menjelaskan dan menerapkan manajemen user pada server. 4. Mahasiswa dapat menjelaskan dan menerapkan manajemen sumber daya dan backup sistem. 5. Mahasiswa dapat menjelaskan dan menerapkan penanganan bencana dan rencana mitigasi terkait server. 6. Mahasiswa dapat menjelaskan dan menerapkan konfigurasi jaringan pada server. 7. Mahasiswa dapat menjelaskan dan menerapkan layanan server yang dibutuhkan seperti web server, application server, directory server, database server, file server, print server, messaging server, mail server, remote access server, dhcp
4.	Keamanan Basis Data	Mahasiswa mampu mengemukakan aspek keamanan yang harus dijaga dalam basis data, baik basis data relasional maupun non relasional. Mahasiswa mampu mengaudit dan menilai keamanan, integritas dan reliabilitas suatu sistem basis data.	1. Mahasiswa mampu merinci control akses dalam basis data. 2. Mahasiswa mampu merinci dan menerapkan standar keamanan basis data relasional. 3. Mahasiswa mampu merinci dan menerapkan standar keamanan basis data non relasional. 4. Mahasiswa mampu mengklasifikasi tingkat keamanan suatu sistem basis data. 5. Mahasiswa mampu menilai dan mengaudit suatu sistem basis data
5.	Interkoneksi Jaringan	Mahasiswa mampu mengidentifikasi prinsip kerja, menganalisa permasalahan, serta melakukan manajemen terhadap Jaringan Komputer yang lebih lanjut.	1. Mahasiswa mampu menjelaskan konsep Switching pada Jaringan Komputer serta keamanannya. 2. Mahasiswa mampu menerapkan konsep VLAN dan Inter-VLAN serta beberapa teknologi yang mendukungnya. 3. Mahasiswa mampu membangun Routing Dinamik. 4. Mahasiswa mampu mengkonfigurasi keamanan jaringan seperti ACL dan NAT. 5. Mahasiswa mampu membangun WLAN serta keamanannya. 6. Mahasiswa mampu menganalisis QoS performa jaringan
6.	Pemrograman Berorientasi Objek	Mahasiswa mampu menjelaskan dan menerapkan konsep OOP pada pemrograman berbasis web dan mengenal celah keamanan pada web dan mengatasinya.	1. Mahasiswa mampu untuk meningkatkan organisasi, keterbacaan, dan pemeliharaan kode dengan menggunakan konsep kelas dan objek. 2. Mahasiswa mampu mengimplementasikan konsep dasar pemrograman berorientasi objek, yang

			meliputi konsep kelas, objek, property, method, Encapsulation, Inheritance, Abstraction, dan Polymorphism. 3. Mahasiswa mampu menjelaskan dan menerapkan prinsip SOLID. 4. Mengimplementasikan aplikasi yang terhubung dengan basis data berdasarkan paradigma orientasi objek dan secure coding.

11. Komunikasi antara Manajer Proyek dan Klien

Fase/Proses	Pertanyaan/Komentar	Jawaban	Catatan
…	…	…	…

12. Monitoring dan Evaluasi

Monitoring dan evaluasi dilakukan dalam waktu minimal 1 (satu) minggu sekali oleh Manajer Proyek secara Daring atau Luring.

13. Riwayat Perubahan Proyek yang akan ditangani

No. Revisi/tanggal	Deskripsi Perubahan	*Originator*
…	…	…

Tanda Tangan Persetujuan
Batam, 28/09/2025

Maidel Fani, S.Pd., M.Kom
Klien

Muhammad Idris, S.Tr., M.Tr.Kom
Manajer Proyek

Ahmad Hamim Thohari, S.S.T., M.T.
Ketua Jurusan Teknik Informatika

Maidel Fani, S.Pd., M.Kom.
KPS Rekayasa Keamanan Siber