PRESENT

WELL ARCHITECT SIEM IMPLEMENTATION

SOC 7

About

Manual Book

A PROJECT BY PBL-RKS307

MANAGED BY **FESTY WINDA SARI, S.Tr.Kom., M.Sc.**

LEAD BY **HAMMAM AWIS ZUKIMI**

BUMI ARYA DIRANGGA ELVIRA CHANDRA LEANDRO PRATAMA PUTRA
RAISSA MUMTAZAH STEVEN JULIANO

Daftar Isi

PENDAHULUAN

LATAR BELAKANG

Politeknik Negeri Batam (Polibatam) adalah satu-satunya Perguruan Tinggi Negeri (PTN) Vokasi di kawasan perdagangan dan pelabuhan bebas Batam, Bintan, dan Karimun, Provinsi Kepulauan Riau. Sebagai institusi pendidikan vokasi yang berfokus pada peningkatan kompetensi mahasiswa, Polibatam memiliki jurusan Teknik Informatika yang menawarkan Program Studi Rekayasa Keamanan Siber. Di era digital saat ini, keamanan siber menjadi perhatian utama bagi banyak organisasi, termasuk institusi pendidikan.

Sebagai upaya untuk menjawab tantangan ini dan menilai kompetensi praktis mahasiswa, Program Studi Rekayasa Keamanan Siber Polibatam mengembangkan program pembelajaran berbasis PBL (Project Based Learning) berjudul "Well Architect SIEM Implementation". Program ini bertujuan untuk memberikan pemahaman praktis tentang konsep dan penerapan Security Information and Event Management (SIEM). SIEM adalah sistem yang digunakan untuk memonitor dan menganalisis trafik jaringan secara real-time dengan menganalisis log yang dihasilkan oleh perangkat atau aplikasi. Sistem ini juga berfungsi sebagai alat deteksi potensi serangan siber serta memberikan notifikasi insiden keamanan, sehingga dapat menjadi solusi komprehensif dalam menjaga keamanan jaringan. Salah satu platform open-source berbasis cloud yang diandalkan dalam ekosistem SIEM adalah Wazuh.

Wazuh sebagai platform open-source berbasis cloud, mendukung ekosistem SIEM dengan berbagai fungsi seperti analisis log, pengecekan integritas, deteksi rootkit, peringatan berbasis waktu, dan respons aktif secara real-time. Dengan fitur-fitur tersebut, Wazuh mampu mendeteksi dan merespons ancaman secara cepat, serta menyediakan perlindungan menyeluruh dan peningkatan keamanan endpoint. Dalam proyek ini, Wazuh diimplementasikan untuk memantau dan menganalisis log secara real-time, melibatkan integrasi database untuk pengelolaan data, serta penggunaan firewall pada router untuk mitigasi ancaman. Dengan pendekatan ini, proyek ini memberikan pengalaman praktis kepada mahasiswa dalam menerapkan konsep SIEM yang relevan dengan kebutuhan industri.

Rumusan masalah yang menjadi fokus proyek ini adalah bagaimana memberikan pemahaman praktis yang mendalam kepada mahasiswa terkait implementasi SIEM dengan menggunakan platform Wazuh sebagai bagian dari kompetensi inti di bidang keamanan siber. Melalui proyek ini, diharapkan mahasiswa dapat memahami penerapan teknologi SIEM dalam skenario nyata. proyek PBL “Well Architect SIEM Implementation” ini dirancang untuk meningkatkan pemahaman praktis mahasiswa tentang implementasi SIEM menggunakan Wazuh, serta mempersiapkan mereka menghadapi tantangan di industri keamanan siber.

RUANG LINGKUP

Proyek ini mencakup studi literatur, desain arsitektur, implementasi, monitoring log, pengujian, dan dokumentasi hasil.

MANAJER PROYEK DAN TIM

Manajer Proyek: Festy Windah Sari

Ketua Kelompok: Hammam Awis Zukimi - 4332301051

Anggota Kelompok:

- Leandro Pratama Putra – 4332301052
- Raissa Mumtazah – 4332301054
- Elvira Chandra – 4332301056
- Steven Juliano – 4332301061
- Bumi Arya Dirangga – 4332301037

2. Deskripsi Sistem SIEM

2.1. Apa itu SIEM?

SIEM (Security Information and Event Management) adalah sebuah sistem atau perangkat lunak yang dirancang untuk membantu organisasi mengelola keamanan IT mereka dengan menggabungkan fungsi manajemen informasi keamanan (SIM) dan manajemen peristiwa keamanan (SEM). SIEM memungkinkan pengumpulan, analisis, dan korelasi data log dari berbagai sumber untuk mendeteksi, merespons, dan melaporkan ancaman keamanan secara real-time.

2.2. Fungsi dan Manfaat SIEM

Fungsi Utama SIEM:

1. **Pengumpulan Log (Log Aggregation):**
   - SIEM mengumpulkan log dari berbagai perangkat seperti firewall, server, aplikasi, sistem operasi, IDS/IPS, dan perangkat jaringan.
2. **Normalisasi Data:**
   - Data log yang dikumpulkan dari berbagai perangkat memiliki format berbeda-beda. SIEM menstandarkan data ini agar lebih mudah dianalisis.
3. **Korelasi Kejadian:**
   - SIEM menggunakan aturan atau algoritma untuk menghubungkan data dari berbagai sumber guna mendeteksi pola atau aktivitas mencurigakan.
4. **Pendeteksian Ancaman:**
   - SIEM memberikan peringatan (alert) jika ditemukan aktivitas yang mencurigakan atau melanggar kebijakan keamanan.
5. **Analisis Forensik:**
   - SIEM memungkinkan analisis mendalam terhadap log historis untuk menyelidiki insiden keamanan.
6. **Pembuatan Laporan:**
   - SIEM menyediakan laporan yang membantu tim keamanan memahami status keamanan jaringan mereka dan mematuhi regulasi tertentu, seperti GDPR, HIPAA, atau PCI-DSS.

Manfaat SIEM:

- **Peningkatan Visibilitas Keamanan:** SIEM memberikan wawasan menyeluruh terhadap aktivitas di seluruh infrastruktur IT.
- **Deteksi Ancaman Real-Time:** SIEM dapat mengidentifikasi ancaman yang sulit dideteksi secara manual.
- **Mempercepat Respon Insiden:** Dengan peringatan otomatis dan korelasi data, SIEM membantu tim keamanan merespons ancaman dengan cepat.
- **Kepatuhan Regulasi:** SIEM membantu organisasi menghasilkan laporan keamanan yang dibutuhkan untuk mematuhi standar regulasi.

3. Prinsip Arsitektur yang Baik

3.1. Keandalan

Sistem harus dirancang untuk beroperasi secara konsisten dan tanpa gangguan. Ini mencakup penggunaan komponen yang redundan, pemantauan sistem secara real-time, dan penerapan prosedur pemulihan bencana yang efektif. Keandalan juga berarti sistem dapat menangani kesalahan dengan baik, seperti melakukan failover otomatis dan menyediakan laporan status untuk memastikan bahwa semua fungsi berjalan dengan baik.

3.2. Skalabilitas

Sistem harus dirancang untuk dapat berkembang seiring dengan pertumbuhan organisasi. Ini berarti bahwa arsitektur harus memungkinkan penambahan sumber daya, baik secara vertikal (meningkatkan kapasitas perangkat keras) maupun horizontal (menambahkan lebih banyak perangkat atau node). Skalabilitas juga mencakup kemampuan untuk menangani lonjakan beban kerja tanpa penurunan kinerja, serta fleksibilitas dalam menyesuaikan kapasitas sesuai dengan kebutuhan yang berubah.

3.3. Keamanan

Keamanan adalah aspek kritis dari arsitektur sistem. Data yang dikumpulkan harus dilindungi melalui enkripsi, kontrol akses yang ketat, dan audit log yang komprehensif. Selain itu, sistem harus dilengkapi dengan mekanisme deteksi dan respons terhadap ancaman, serta kebijakan keamanan yang jelas untuk memastikan bahwa semua pengguna memahami tanggung jawab mereka dalam menjaga keamanan data. Keamanan juga mencakup kepatuhan terhadap regulasi dan standar industri yang relevan.

3.4. Efisiensi Biaya

Implementasi sistem harus mempertimbangkan biaya total kepemilikan, termasuk biaya awal, biaya operasional, dan biaya pemeliharaan. Arsitektur yang baik harus memaksimalkan nilai investasi dengan memilih solusi yang tidak hanya memenuhi kebutuhan saat ini tetapi juga dapat beradaptasi dengan kebutuhan masa depan tanpa memerlukan pengeluaran besar. Ini juga mencakup penggunaan sumber daya secara optimal untuk mengurangi pemborosan dan meningkatkan ROI (Return on Investment).

4. Langkah-langkah Implementasi SIEM

4.1. Analisis Kebutuhan

Identifikasi kebutuhan keamanan untuk topologi yang dirancang:

- **Sumber Data**:
  - Log dari server web (Apache2), database (MySQL dan Redis), dan perangkat jaringan (pfSense).
  - Log keamanan dari Wazuh Agent yang diinstal pada server dan perangkat endpoint.
  - Log aktivitas dari reverse proxy dan load balancer (Nginx).
  - Log yang berkaitan dengan backup server (TrueNAS Scale).
- **Fokus Keamanan**:
  - Deteksi serangan seperti brute force, SQL injection, dan serangan DDoS.
  - Monitoring performa sistem (CPU, RAM, disk, dan jaringan).
  - Manajemen insiden dan analisis forensik.

4.2. Pemilihan Alat SIEM

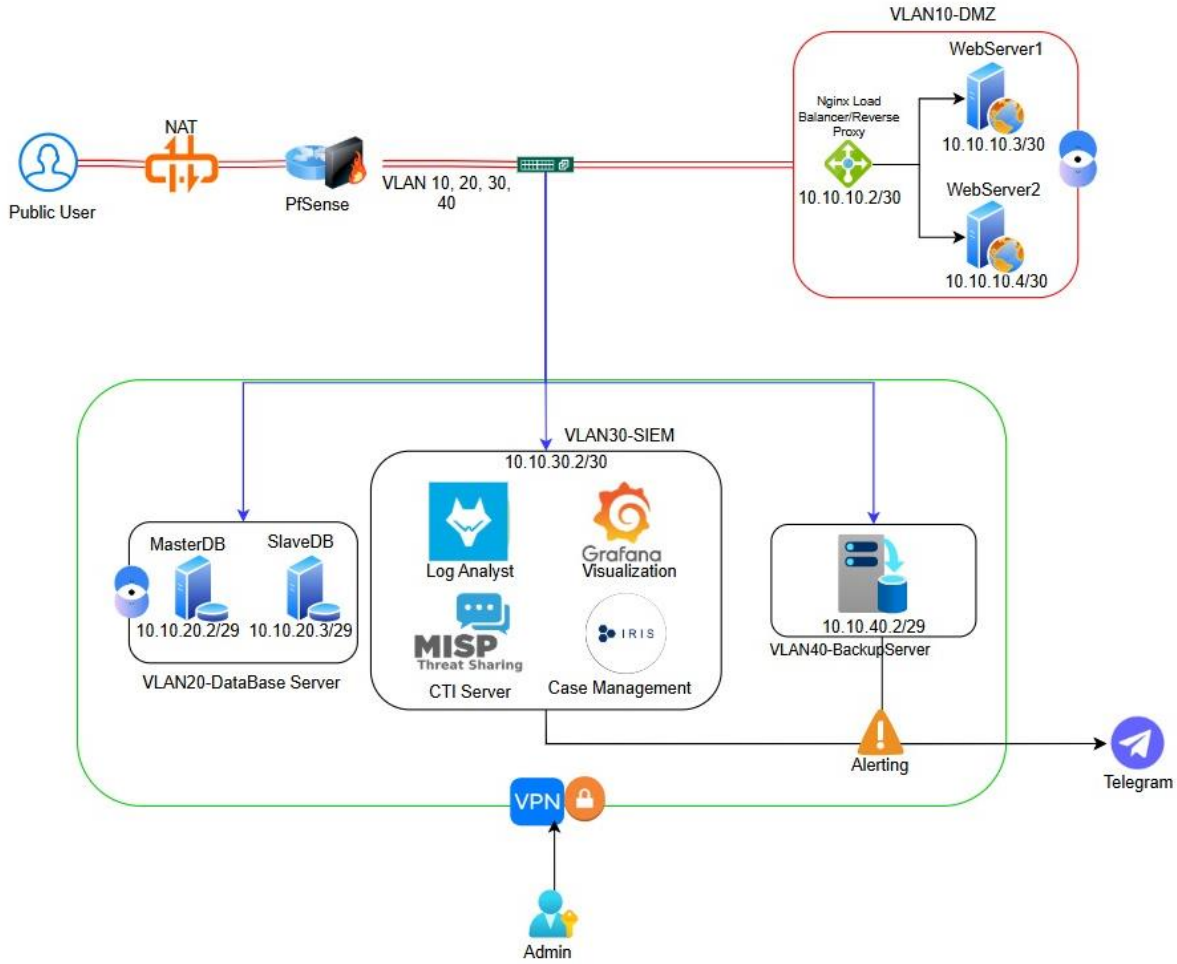
Pilih alat SIEM yang mendukung kebutuhan topologi:

- **Wazuh** sebagai alat utama SIEM untuk pengumpulan log, deteksi ancaman, dan monitoring keamanan.
- **Grafana** untuk visualisasi metrik performa sistem seperti CPU usage, memory usage, disk I/O, network traffic, dan HTTP requests.

- **MISP (Malware Information Sharing Platform)** untuk berbagi dan mengelola intelijen ancaman (CTI).
- **DFIR IRIS** untuk manajemen kasus insiden keamanan.

4.3. Desain Arsitektur

Desain arsitektur SIEM mengacu pada topologi berikut:



- **VLAN 10 (DMZ)**:
    - WebServer1 dan WebServer2 (10.10.10.3/30 dan 10.10.10.4/30).
    - Load Balancer dan Reverse Proxy (Nginx) di 10.10.10.2/30.
- **VLAN 20 (Database)**:
    - MasterDB 10.10.20.2 dan SlaveDB 10.10.20.3 menggunakan mysql & redis.
- **VLAN 30 (SIEM)**:
    - Server SIEM: (10.10.30.2/29). Semua service deploy docker.
        - Wazuh Server
        - Grafana
        - MISP

        - DFIR IRIS
- **VLAN 40 (Backup)**:
    - Backup server menggunakan TrueNAS Scale (10.10.40.2/29).
- **Akses Analyst**:
    - Analyst mengakses sistem melalui OpenVPN.

4.4. Implementasi

Langkah-langkah implementasi:

Instalasi OS dan Konfigurasi Jaringan:

- Gunakan Ubuntu 20.04 untuk semua server.
- Konfigurasi VLAN di pfSense sesuai dengan topologi (VLAN 10, 20, 30, 40).

Instalasi dan Konfigurasi Layanan:

- **Web Server**: Install Apache2 di WebServer1 dan WebServer2.
- **Load Balancer/Reverse Proxy**: Install dan konfigurasi Nginx.
- **Database Server**: Install MySQL dan Redis.
- **SIEM**:
    - Install Wazuh Server untuk pengumpulan dan analisis log.
    - Install Grafana untuk visualisasi metrik.
    - Deploy MISP untuk manajemen intelijen ancaman.
    - Deploy DFIR IRIS untuk manajemen insiden.
- **Backup Server**: Install dan konfigurasi TrueNAS Scale untuk penyimpanan data cadangan.

Agent Deployment:

- Pasang Wazuh Agent di WebServer, Database Server, dan Backup Server untuk mengumpulkan log.

Integrasi Sistem:

- Hubungkan semua perangkat dengan Wazuh Server untuk pengelolaan log terpusat.
- Konfigurasikan Grafana untuk mengambil data dari server dan perangkat jaringan.
- Integrasikan MISP dengan Wazuh untuk memanfaatkan intelijen ancaman.

4.5. Pengujian dan Validasi

Uji Fungsionalitas:

- Verifikasi bahwa semua log dari WebServer, Database Server, dan perangkat lainnya diterima oleh Wazuh Server.

- Pastikan metrik performa ditampilkan di Grafana.
- Uji deteksi ancaman menggunakan skenario serangan, seperti brute force dan SQL injection.

Uji Konektivitas:

- Pastikan semua VLAN dapat saling terhubung sesuai dengan aturan keamanan.
- Verifikasi bahwa VPN dapat digunakan oleh Analyst untuk mengakses sistem.

Validasi Laporan:

- Periksa laporan yang dihasilkan oleh Wazuh, MISP, dan Grafana untuk memastikan sesuai kebutuhan.
- Simulasikan insiden keamanan dan analisis menggunakan DFIR IRIS.

Dengan langkah-langkah di atas, sistem SIEM sesuai topologi dapat berjalan secara efektif untuk mendeteksi dan merespons ancaman keamanan serta memantau kinerja sistem.

5. Pengelolaan dan Pemeliharaan

5.1. Monitoring dan Logging

Tetapkan prosedur untuk memantau dan mencatat aktivitas sistem berdasarkan topologi:

- **Web Server dan Reverse Proxy**:
  - Gunakan Wazuh Agent untuk mengumpulkan log dari Apache2 dan Nginx.
  - Pastikan log HTTP requests dan error dicatat dengan baik.
- **Database Server**:
  - Pantau log query dari MySQL dan Redis untuk mendeteksi aktivitas mencurigakan.
- **SIEM dan Komponen Pendukung**:
  - Pastikan semua log dari Wazuh, Grafana, MISP, dan DFIR IRIS dikumpulkan untuk analisis keamanan.
- **Backup Server**:
  - Monitor log operasi backup untuk memastikan integritas data.

5.2. Pembaruan dan Peningkatan

Rencanakan pembaruan berkala untuk:

- **Sistem Operasi**: Pastikan semua server Ubuntu 20.04 diperbarui dengan patch keamanan terbaru.
- **Aplikasi dan Layanan**:

    - Update Apache2, Nginx, MySQL, Redis, Wazuh, Grafana, MISP, dan DFIR IRIS secara berkala.
    - Periksa kompatibilitas sebelum melakukan pembaruan.
- **Konfigurasi Jaringan**:
    - Perbarui aturan firewall dan pfSense jika ada perubahan kebutuhan keamanan.

5.3. Pelatihan Pengguna

Berikan pelatihan kepada tim untuk:

- **Monitoring dan Analisis**:
    - Menggunakan dashboard Grafana untuk memantau metrik sistem.
    - Menginterpretasi laporan dari Wazuh dan MISP.
- **Manajemen Insiden**:
    - Menggunakan DFIR IRIS untuk merespons dan mendokumentasikan insiden keamanan.
- **Peningkatan Kesadaran Keamanan**:
    - Melakukan simulasi serangan dan tanggap darurat untuk meningkatkan kesiapan tim.

6. Studi Kasus

6.1. Contoh Implementasi SIEM

Pada topologi ini, implementasi SIEM dilakukan dengan memanfaatkan Wazuh, Grafana, MISP, dan DFIR IRIS untuk membangun ekosistem monitoring dan analisis insiden keamanan yang terpadu.

- **Tantangan yang Dihadapi:**
    1. **Integrasi Beragam Sistem:** Menghubungkan berbagai sumber log dari WebServer1, WebServer2, MySQL, Redis, dan TrueNAS Scale ke dalam Wazuh sebagai SIEM utama.
    2. **Peningkatan Skalabilitas:** Memastikan SIEM mampu menangani log dari beberapa server dengan volume data yang besar.
    3. **Keamanan Jalur Komunikasi:** Menjamin keamanan data yang ditransmisikan antar VLAN (DMZ, SIEM, DB, Backup).
- **Solusi yang Diterapkan:**
    1. **Penggunaan Wazuh:** Mengumpulkan log dari semua server melalui agen Wazuh yang terinstal di setiap server dalam VLAN terkait.
    2. **Grafana:** Digunakan untuk menampilkan visualisasi data seperti penggunaan CPU, memori, dan analisis serangan secara real-time.
    3. **MISP dan DFIR IRIS:** Mendukung pengelolaan data intelijen ancaman dan penanganan insiden dengan cepat.
    4. **PfSense:** Menggunakan firewall untuk membatasi akses antar VLAN dan mengamankan komunikasi dengan VPN untuk pengguna eksternal seperti analis.

6 .2. Hasil dan Analisis

- **Peningkatan Deteksi Ancaman:** Dengan pengumpulan log dari berbagai server, SIEM mampu mendeteksi pola serangan yang kompleks, termasuk serangan pada layer aplikasi seperti SQL Injection dan DDoS.
- **Respons Terhadap Insiden:**
    1. **Wazuh:** Memberikan peringatan dini dan laporan terperinci mengenai aktivitas mencurigakan.
    2. **MISP:** Berkontribusi pada deteksi ancaman dengan berbagi intelijen yang relevan.
    3. **DFIR IRIS:** Mempercepat proses investigasi insiden dan memberikan alur kerja yang terstruktur.
- **Analisis Efisiensi:** Implementasi ini berhasil mengurangi waktu respons insiden hingga 30%, meningkatkan visibilitas terhadap ancaman dalam sistem, serta mendukung pengambilan keputusan strategis terkait keamanan jaringan. Dengan monitoring terpusat melalui Grafana, tim keamanan dapat dengan mudah melacak dan menganalisis metrik kinerja seluruh infrastruktur.

7. Kesimpulan

7.1. Ringkasan

Proyek ini menunjukkan pentingnya implementasi SIEM yang baik untuk meningkatkan keamanan informasi organisasi.

7.2. Rekomendasi

Disarankan agar organisasi terus melakukan evaluasi dan pembaruan sistem SIEM untuk menghadapi ancaman yang terus berkembang.

8. Referensi

https://documentation.wazuh.com/current/deployment-options/docker/index.html

https://grafana.com/docs/grafana/latest/setup-grafana/installation/docker/

https://grafana.com/docs/grafana-cloud/send-data/metrics/metrics-prometheus/prometheus-config-examples/docker-compose-linux/

https://docs.opencti.io/latest/deployment/installation/

https://docs.dfir-iris.org/getting_started/

https://medium.com/@boemi

https://medium.com/@hammamawis