SNIV: SEMINAR NASIONAL INOVASI VOKASI
eISSN 2830-0343

Mengenal SIEM dan SOAR: Pilar Utama Keamanan Informasi Modern

Imola Anggraini[1*] dan Dandun Widhiantoro[1]

1. Program Studio Broadband Multimedia, Jurusan Teknik Elektro, Politeknik Negeri Jakarta, Depok, 16425, Indonesia

**E-mail: imola.anggraini.te21@mhsw.pnj.ac.id*

Abstrak

Dalam era digital saat ini, organisasi membutuhkan sistem pertahanan yang fleksibel dan efektif. *Security Information and Event Management* (SIEM) dan *Security Orchestration, Automation, and Response* (SOAR) adalah dua pilar utama sistem keamanan kontemporer. Studi ini bertujuan untuk membandingkan fungsi, keunggulan, dan keterbatasan implementasi nyata keduanya. Hasil penelitian menunjukkan bahwa SIEM unggul sebagai dasar sistem keamanan karena mereka dapat mengumpulkan, mengorelasikan, dan menganalisis data *log* dari berbagai sumber secara *real time* serta memenuhi semua kebutuhan untuk kepatuhan dan deteksi dini. SIEM juga lebih mudah diimplementasikan dan mempengaruhi visibilitas dan kendali keamanan organisasi. Sementara SOAR memiliki tingkat efisiensi yang tinggi melalui otomasi respons insiden, tetapi kinerjanya sangat bergantung pada ketepatan dan kelengkapan data yang dikumpulkan, serta bagaimana sistemnya diintegrasikan. Karena itu, artikel ini merekomendasikan implementasi SIEM yang matang sebagai langkah awal sebelum mengadopsi SOAR karena SIEM memberikan dasar data dan konteks yang dibutuhkan untuk orkestrasi otomatis yang optimal. Dengan demikian, SIEM dianggap sebagai investasi strategis yang lebih penting dan berkelanjutan dalam memperkuat posisi keamanan siber organisasi.

Kata Kunci: Keamanan Siber, SIEM, SOAR, Deteksi Ancaman, Otomatisasi Keamanan

Abstract

In the era of the digital age, organisations need flexible and effective defence systems... Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) are the two main pillars of contemporary security systems. This study aims to compare the functions, advantages, and limitations of their real-world implementations. The results show that SIEMs excel as the foundation of security systems because they can collect, correlate, and analyse log data from multiple sources in real-time and meet all needs for compliance and early detection. SIEMs are also easier to implement and impact an organisation's security visibility and control. While SOAR has a high level of efficiency through incident response automation, its performance is highly dependent on the accuracy and completeness of the data collected, as well as how the systems are integrated. As such, this article recommends a mature SIEM implementation as a first step before adopting SOAR because SIEM provides the data foundation and context needed for optimal automated orchestration. As such, SIEM is considered a more important and sustainable strategic investment in strengthening an organisation's cybersecurity position.

Keywords: Cyber Security, SIEM, SOAR, Threat Detection, Security Automation

1. Pendahuluan

Kebocoran informasi dapat memiliki konsekuensi yang sangat merugikan bagi individu, organisasi, atau bahkan negara. Dalam era digital yang semakin kompleks, keamanan siber menjadi komponen penting bagi perusahaan untuk melindungi aset informasi dari berbagai ancaman yang terus muncul. Dua teknologi utama untuk meningkatkan pertahanan siber adalah *Security Information and Event Management* (SIEM) dan *Security Orchestration, Automation, and Response* (SOAR).

Menurut Wardana (2020:46) SIEM merupakan cara yang digunakan dalam mengatur sebuah jaringan berdasarkan kondisi yang terjadi, dimana dalam implementasi SIEM banyak *tools* yang digunakan. SOAR, di sisi lain, mempercepat waktu tanggap dan meningkatkan efisiensi operasional dengan mengotomatiskan dan mengorkestrasi proses respons terhadap insiden melalui *playbook* otomatis dan integrasi alat keamanan yang komprehensif. Meskipun keduanya saling melengkapi, perbedaan fungsi dan metode ini membuat kita perlu memahami secara menyeluruh manfaat dan kekurangan masing-masing ketika digunakan dalam dunia nyata. Tujuan dari artikel ini adalah untuk membandingkan SIEM dan SOAR dalam hal deteksi, otomatisasi respons, integrasi sistem, dan pengaruh mereka terhadap kinerja operasional keamanan siber. Tujuannya adalah untuk memberi panduan bagi organisasi dalam memilih dan mengintegrasikan teknologi yang tepat untuk memperkuat postur keamanan mereka secara menyeluruh.

2. Metode Penelitian

Metode penelitian yang digunakan untuk mendapatkan pemahaman yang lebih baik tentang konsep, fungsi, dan penerapan teknologi *Security Information and Event Management* (SIEM) dan *Security Orchestration, Automation, and Response* (SOAR) dalam konteks keamanan siber kontemporer, penelitian ini menggunakan pendekatan *review* literatur. Pendekatan kualitatif digunakan untuk menganalisis berbagai sumber pustaka yang relevan.
Sebagai berikut adalah hasil penelitian:

1. Identifikasi dan Seleksi Literatur: Peneliti menggunakan kata kunci seperti “SIEM”, “SOAR”, “*cybersecurity architecture*”, dan “deteksi dan respons ancaman” untuk mengumpulkan literatur dari database ilmiah seperti IEEE *Xplore*, *ScienceDirect*, dan *SpringerLink*, antara sumber lain yang dapat diandalkan. Untuk memastikan relevansi dan kemutakhiran data, literatur yang dipilih berfokus pada publikasi selama lima tahun terakhir (2020–2025).
2. Analisis dan Sintesis Informasi: Literatur yang telah dipilih secara kualitatif dianalisis untuk menemukan kecenderungan, pola, perbandingan teknologi, keuntungan, dan tantangan dalam penggunaan SIEM dan SOAR. Data juga dianalisis secara tematik untuk menentukan hubungan dan peran kedua teknologi dalam sistem keamanan siber kontemporer.
3. Membuat Hasil dan Pembahasan
   Hasil kajian disusun secara sistematis untuk menjelaskan fungsi strategis SIEM dan SOAR dan bagaimana keduanya dapat dimasukkan ke dalam arsitektur keamanan. Mereka juga memiliki kemungkinan untuk meningkatkan deteksi dan tanggapan terhadap ancaman siber. Penelitian ini diharapkan dapat memberikan kontribusi konseptual yang bermanfaat untuk membantu akademisi, praktisi, dan organisasi memahami SIEM dan SOAR sebagai bagian dari sistem keamanan mereka.

3. Pembahasan

3.1 SIEM

Security Information and Event Management (SIEM) merupakan sistem pemantauan yang berfungsi untuk mendeteksi serangan serta merespons insiden keamanan dengan menganalisis *log* dari berbagai *event* yang dikumpulkan secara real time. Sumber data *log* ini bisa berasal dari perangkat seperti IDS, IPS, UTM, router, maupun server. *Log* sendiri berisi catatan aktivitas dari perangkat, termasuk lalu lintas jaringan, kondisi perangkat, dan aktivitas lainnya. Informasi *login* ditampilkan melalui *Syslog*, termasuk proses pemeliharaan, dan jika terdapat ancaman keamanan, perangkat akan menghasilkan *log* sebagai peringatan. SIEM memiliki kemampuan untuk mengelola dan menganalisis kumpulan data dalam jumlah besar, serta mengkorelasikan berbagai peristiwa dari banyak sumber untuk menentukan apakah suatu aktivitas mencurigakan merupakan serangan atau bukan. Umumnya, SIEM menyajikan dua jenis *output* : berupa laporan dan peringatan. Fitur pelaporan pada SIEM akan menampilkan data terkait insiden keamanan, termasuk aktivitas mencurigakan hingga percobaan *login* dan

mengalami kegagalan. Fitur peringatan dapat berlangsung di saat mesin analisa mendeteksi terdapat gerakan mencurigakan, di sisi lain SIEM pun mempercepat deteksi ancaman hingga peringatan keamanan.

Fitur-fitur yang ada pada SIEM antara lain :

a. *Log/Event Collection*, system melakukan pengumpulan *log* dari bermacam-macam tipe *log* , serta sumber lain yang berbeda.
b. *Log analysis*, melakukan pengolahan dan analisa data dari banyak sumber dengan cara *real time* juga menggambarkannya pada sebuah grafik maupun diagram supaya seorang administrator bisa dengan baik mengerti dan melakukan pengambilan keputusan.
c. *Event Correlation*, fitur ini memfasilitasi administrator melakukan peningkatan keamanan dengan memproses jutaan log dengan bersama-sama guna melakukan pendeteksian *anomaly* didalam sistem.
d. *Log Forensics*, SIEM dapat mendukung proses investigasi forensik log dengan menyajikan data atau peristiwa yang mudah dipahami, sehingga memudahkan dalam melacak keberadaan penyusup atau mengidentifikasi sumber masalah dalam sistem.
e. IT *Compliance*, SIEM menyajikan laporan terkait pelanggaran terhadap berbagai standar dan kebijakan keamanan.
f. *Application Log Monitoring*, fitur yang membantu administrator melakukan pemantauan *log* dari aplikasi mereka secara *real time.*
g. *Real Time Alerting*, fitur untuk memberikan peringatan kepada administrator apabila terjadi suatu hal yang mencurigakan pada sistem.
h. *Object Access Auditing*, fitur untuk mengaudit segala aset penting sistem yang ada.
i. *User Activity Monitor*, membantu memantau aktivitas pengguna secara *real time* dan mendeteksi penyalahgunaan hak.
j. *Dashboard*, fitur untuk menampilkan data dan informasi keamanan yang telah diolah.
k. *Reporting*, SIEM menyediakan laporan sesuai dengan standar keamanan yang ada.
l. *File Integrity Monitoring*, memantau apabila terjadi perubahan data yang tidak wajar, penyalahgunaan hak atau akses dari yang tidak berwenang.
m. *System & Device Log Monitoring*, fitur untuk melakukan otomatisasi pemantauan *log* serta analisis sistem dan *log* secara *real time*.

Untuk meningkatkan pemahaman kita tentang penggunaan SIEM dalam mendeteksi dan menangani ancaman keamanan informasi, penelitian sebelumnya telah dilakukan. Tabel 1 menyajikan ringkasan penelitian yang berkaitan dengan penggunaan SIEM, khususnya yang menggunakan Elastic SIEM sebagai alat bantu pemantauan keamanan siber.

Tabel 1. Hasil Studi Literatur SIEM

Referensi	Hasil Studi Literatur Jurnal
[1] Implementasi Security Information and Event Management (SIEM) Pada Lingkungan ITSEC ASIA Menggunakan Elastic SIEM	Fazrin Alfiansyah menulis artikel dalam jurnal "Implementasi Manajemen Informasi dan Peristiwa Keamanan (SIEM) pada Lingkungan ITSEC Asia Menggunakan Elastic SIEM" yang membahas penerapan Elastic SIEM untuk meningkatkan deteksi dan pengawasan serangan siber di jaringan ITSEC Asia. Studi ini menekankan pentingnya menangani ancaman keamanan yang disebabkan oleh kerentanan sistem yang dapat dieksploitasi oleh penyerang. Mengintegrasikan berbagai *log agent* seperti *Suricata*, *Wazuh*, dan *Winlogbeat* ke dalam Elastic SIEM akan membuat pengawasan lebih terkonsentrasi dan efisien. Pengujian dilakukan untuk memastikan kemampuan sistem untuk mendeteksi dan merespons serangan *brute force* secara *real time*. Hasilnya menunjukkan bahwa Elastic SIEM mampu mengidentifikasi serangan *brute force* dan aktivitas penambahan dan penghapusan *user* dengan cepat, yang memudahkan administrator untuk memantau dan mengelola keamanan jaringan secara menyeluruh. Hasilnya menunjukkan bahwa Elastic SIEM dapat dengan cepat mengidentifikasi serangan *brute force* dan aktivitas penambahan dan penghapusan *user*. Ini memudahkan administrator untuk memantau dan mengelola secara menyeluruh keamanan jaringan.
[2] Implementation Of Security Information And	Jurnal yang ditulis oleh M. Reyza Putra Paw dan rekan berjudul "Implementasi Manajemen Informasi dan Peristiwa Keamanan (SIEM) dalam Pengawasan Jaringan di SMA 1 Muhammadiyah Boarding School" membahas penerapan sistem SIEM menggunakan OSSIM

Event Management (Siem) In Monitoring Networks At SMA 1 Muhammadiyah Boarding School	*AlienVault* untuk memantau aktivitas dan status perangkat yang terhubung dalam jaringan sekolah. Melalui antarmuka *web* yang mudah diakses, sistem ini memberikan informasi *log* layanan dan *event* keamanan secara *real time*, membantu administrator jaringan mengetahui apakah perangkat dalam keadaan aktif (*UP*) atau tidak (*DOWN*). Meskipun beberapa serangan tertentu seperti *brute force* tidak terdeteksi, pengujian sistem menunjukkan bahwa OSSIM *AlienVault* berhasil melakukan monitoring jaringan, mendeteksi 27 aset jaringan, dan menyediakan *log* peristiwa yang bermanfaat untuk analisis keamanan. Studi ini menemukan bahwa penerapan SIEM sangat membantu dalam mempermudah pengelolaan dan pemantauan jaringan di SMA Muhammadiyah Boarding School. Studi ini juga menyarankan pengembangan tambahan dengan menambah sensor dan mendefinisikan IP *address* aset untuk membuat identifikasi perangkat lebih akurat dan membuat pengawasan lebih mudah bagi administrator.
[3] Perancangan dan Pengembangan Aplikasi Deteksi Anomali pada Jaringan Internet Gedung Disaster Recovery Center Badan Diklat Kejaksaan RI dengan Implementasi Sistem Manajemen Informasi dan Keamanan (SIEM) Berbasis Web	Jurnal "Perancangan dan Pengembangan Aplikasi Deteksi Anomali pada Jaringan Internet Gedung Disaster Recovery Center Badan Diklat Kejaksaan RI dengan Implementasi Sistem Manajemen Informasi dan Keamanan (SIEM) Berbasis Web" membahas pengembangan aplikasi berbasis SIEM yang menggunakan Python. Aplikasi ini membantu administrator jaringan memantau alur komunikasi dan menemukan ancaman yang mungkin terjadi pada jaringan internet Gedung Disaster Recovery Center. Dengan mengumpulkan dan menganalisis data *log* secara *real time* dari berbagai sumber, termasuk perangkat keras, aplikasi, dan jaringan, sistem ini dapat mendeteksi anomali berbahaya dan memberikan informasi terkini tentang kondisi jaringan. Selain itu, aplikasi ini memiliki *dashboard* berbasis *web* yang memudahkan pemantauan dan pelaporan hasil pengawasan kepada pimpinan. Penelitian menunjukkan bahwa penerapan SIEM meningkatkan kemampuan pengawasan lalu lintas jaringan dan perlindungan aset informasi, serta memudahkan respons cepat terhadap ancaman siber. Oleh karena itu, melalui otomatisasi deteksi anomali dan pemantauan berkelanjutan, sistem ini berkontribusi secara signifikan pada peningkatan keamanan jaringan di lingkungan Badan Diklat Kejaksaan RI.
[4] STRATEGI IMPLEMENTASI SIEM UNTUK MENGURANGI RISIKO TERHADAP KEBOCORAN INFORMASI	Jurnal "Strategi Implementasi SIEM untuk Mengurangi Risiko Kebocoran Informasi" membahas metode dan langkah-langkah penting dalam penerapan Sistem Manajemen Informasi dan Peristiwa (SIEM) untuk meningkatkan keamanan data dan meminimalkan kemungkinan kebocoran informasi di perusahaan. Konfigurasi korelasi yang didasarkan pada aturan adalah strategi utama yang dipilih untuk mempermudah penyaringan *log* yang masuk ke dalam Manajemen Log Pusat (CLM), sehingga hanya data yang relevan yang dianalisis secara menyeluruh. Selain itu, ini juga membantu menemukan sumber data yang lengkap, termasuk perangkat jaringan, server, aplikasi, dan *endpoint*. Jurnal ini juga menekankan betapa pentingnya standarisasi dan normalisasi data untuk melakukan analisis korelasi dan mendeteksi pola serangan atau aktivitas mencurigakan lebih awal. Selain itu, untuk memastikan respons insiden yang cepat dan tepat sasaran, aturan yang disesuaikan dengan kebutuhan keamanan organisasi dan dipantau secara teratur sangat penting. Selain itu, implementasi SIEM yang efektif harus mempertimbangkan skalabilitas dan integrasi dengan infrastruktur yang ada untuk memungkinkan pengembangan data dan perubahan lanskap ancaman. Dengan menggunakan pendekatan ini, organisasi dapat meningkatkan kemampuan mereka untuk mendeteksi dan menangani kebocoran data secara *real time*, memperkuat keamanan mereka, dan mengurangi kerugian yang dapat disebabkan oleh kegagalan keamanan.
[5] Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server	Jurnal Huelilik Dyan Heluka dan Wiwin Sulistyo berjudul "Perancangan dan Implementasi Manajemen Informasi dan Peristiwa Keamanan (SIEM) pada Layanan Virtual Server" membahas penerapan SIEM dengan *platform open source* Wazuh untuk meningkatkan keamanan layanan V*irtual Private Server* (VPS). SIEM dimaksudkan untuk memudahkan deteksi serangan secara cepat dan terpusat dengan mengumpulkan, menormalisasi, dan mengagregasi *log* dari berbagai sumber internal dan eksternal, seperti kontainer, sistem operasi, dan perangkat jaringan. Serangan pada aplikasi *web* dan protokol SSH, termasuk serangan *brute force* dan *web attack*, adalah fokus utama penelitian ini. Implementasi mampu mendeteksi serangan yang sebelumnya tidak teridentifikasi dan menampilkan data *log* yang terorganisir dalam dashboard yang menarik. Studi tersebut juga menekankan bahwa administrator dan tim keamanan harus berpartisipasi secara aktif dalam pembuatan aturan

	SIEM yang terus diperbarui agar respons terhadap ancaman tetap efektif. Singkatnya, Wazuh sebagai alat SIEM open source terbukti membantu melacak dan menemukan masalah keamanan pada layanan VPS. Dengan demikian, ada kemungkinan untuk pengembangan lebih lanjut melalui integrasi menggunakan perangkat jaringan misalnya *firewall* guna melakukan pengawasan lalu lintas dengan lebih mendetail

3.2 SOAR

Security Orchestration Automation and Response merupakan serangkaian layanan yang mengkoordinasikan dan mengotomatiskan pencegahan ancaman dan respon suatu kejadian. SOAR menawarkan keunggulan utama dalam meningkatkan efisiensi, kecepatan respons, ketersediaan sistem, serta kestabilan operasional dalam keamanan siber. Alat SOAR mampu menyatukan berbagai perangkat dan aplikasi keamanan yang digunakan oleh perusahaan, sehingga tim keamanan bisa mengotomatiskan proses penanganan insiden secara menyeluruh. Hal ini membantu mempercepat waktu dari saat pelanggaran terdeteksi hingga penyelesaiannya. SOAR sendiri dibangun di atas tiga komponen utama, yakni:

A. Orkestrasi mengacu pada pembentukan koneksi antara perangkat keamanan internal dan eksternal, termasuk perangkat siap pakai dan integrasi khusus. Hal ini memungkinkan organisasi untuk menangani inventaris perangkat keamanan dan integrasi pihak ketiga yang terus bertambah.

B. Otomatisasi, menyiapkan buku pedoman dan alur kerja yang dipicu oleh insiden atau aturan. Ini dapat digunakan untuk mengelola peringatan dan menyiapkan tindakan responsif. Meskipun sangat sulit untuk menerapkan otomatisasi keamanan menyeluruh, dengan sedikit campur tangan manusia, banyak tugas dapat diotomatisasi.

C. Respons Insiden, Tindakan otomatis terhadap insiden.

Setelah memahami komponen utama dari SOAR yang meliputi orkestrasi, otomatisasi, dan respons insiden, penting untuk melihat bagaimana penerapannya telah dilakukan pada berbagai studi sebelumnya. Studi literatur ini memberikan gambaran implementasi SOAR dengan pendekatan teknologi terkini, termasuk integrasi kecerdasan buatan yang mampu meningkatkan efektivitas dalam mendeteksi dan merespons ancaman siber secara otomatis. Ini adalah ringkasan hasil penelitian literatur terkait SOAR di dalam table 2 :

Tabel 2. Hasil Studi Literatur SOAR

Referensi	Hasil Studi Literatur
[6] KECERDASAN BUATAN UNTUK SECURITY ORCHESTRATION,AUTOMATION AND RESPONSE:TINJAUAN CAKUPAN	Studi menunjukkan bahwa dengan memasukkan AI ke dalam SOAR, proses respons insiden menjadi lebih mudah dan tim keamanan dapat berkonsentrasi pada tugas strategis karena memberikan data intelijen ancaman yang kaya dan otomatisasi orkestrasi dinamis, termasuk pengaturan *honeypot* secara fleksibel untuk memancing dan mengumpulkan informasi serangan. Jurnal "Kecerdasan Buatan untuk Security Orchestration, Automation and Response: Tinjauan Cakupan" membahas peran penting kecerdasan buatan (AI) dalam meningkatkan efektivitas sistem SOAR untuk deteksi dan respons ancaman siber secara otomatis dan *real time*. AI dan machine learning membantu mengotomatiskan analisis data, mendeteksi serangan seperti DDoS dan *botnet*, serta mengurangi beban kerja tim keamanan dengan mempercepat respons insiden. Selain itu, AI mendukung orkestrasi dinamis dan penggunaan *honeypot* adaptif untuk mengumpulkan intelijen ancaman lebih efektif. Meskipun terdapat beberapa keterbatasan, integrasi AI dalam SOAR terbukti memperkuat kemampuan pertahanan siber organisasi dengan meningkatkan kecepatan dan akurasi deteksi serta respons terhadap serangan.
[7] Perancangan Open Source Security Orchestration Automation and Respon Menggunakan	Jurnal ini membahas tentang solusi untuk masalah pengamanan lalu lintas data pada jaringan padat yang rentan terhadap serangan siber adalah sistem otomatisasi pemilahan paket yang bergantung pada sinkronisasi data pada *Database Profil* IP. Sistem ini menggunakan program MQTT *Collector* berbasis *Python* untuk mendaftar dan mendapatkan data profiling IP secara *real time* dari *Database Profil* IP, yang kemudian digunakan sebagai dasar untuk pemilahan paket data yang diterima. Untuk menguji implementasi sistem, router Mikrotik RB951Ui-2HnD digunakan untuk menyimpan rekam jejak pemblokiran di *MongoDB*.

Wazuh Open Source Security Platform Thehive	Alamat IP yang diidentifikasi sebagai sumber *malware* dengan skor di atas ambang batas otomatis diblokir dan dimasukkan ke dalam *block list*. Dengan delay 30 detik yang ideal, sistem ini dapat melakukan pengecekan dan pembaruan data secara berkala dan mengelola data blokir selama 30 hari, yang kemudian dirilis dan dicatat dalam log. Ini meningkatkan responsivitas dan efektivitas pencegahan serangan secara otomatis dan *real time* pada level perangkat jaringan.
[8] Information Security Systems Design Using SIEM, SOAR and Honeypot	Menurut jurnal "Desain Sistem Keamanan Informasi dengan SIEM, SOAR, dan Honeypot", SOAR memiliki kemampuan untuk meningkatkan otomatisasi dan orkestrasi respons terhadap insiden keamanan, tetapi ada beberapa keterbatasan yang harus diperhatikan. SOAR memiliki kelemahan besar ketika diintegrasikan dengan berbagai sistem keamanan lain, seperti SIEM dan honeypot, yang membutuhkan konfigurasi dan pengawasan yang rumit agar dapat berjalan dengan baik. Selain itu, SOAR tidak berfungsi sebagai pengganti strategi keamanan lengkap, sebaliknya, itu berfungsi sebagai pelengkap yang sangat bergantung pada alat keamanan yang terintegrasi dan data intelijen ancaman yang berkualitas tinggi. Selain itu, mengoperasikan dan memelihara platform SOAR membutuhkan keterampilan teknis yang memadai, sehingga organisasi dengan sumber daya terbatas mungkin menghadapi kesulitan dalam implementasi dan pengelolaannya. Jurnal ini juga menekankan bahwa meskipun SOAR mengotomatisasi banyak proses, peran analis manusia tetap penting untuk membuat keputusan yang tepat dan menyesuaikan diri dengan ancaman baru. Oleh karena itu, meskipun SOAR dapat mempercepat deteksi dan respons terhadap insiden, efektivitasnya sangat bergantung pada integrasi yang baik, sumber daya manusia yang berkualitas tinggi, dan strategi keamanan yang menyeluruh.
[9] Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS	Jurnal "Evaluating Modern Intrusion Detection Methods in the Face of Gen V Multi-Vector Attacks with Fuzzy AHP-TOPSIS" mengkaji berbagai teknik deteksi intrusi modern, termasuk Security Orchestration, Automation, and Response (SOAR), dalam menghadapi serangan siber kompleks Gen V Multi-Vector. Penelitian ini menggunakan metode Fuzzy AHP dan TOPSIS untuk mengevaluasi elemen seperti akurasi deteksi, adaptabilitas, skalabilitas, dampak sumber daya, waktu respons, dan tingkat otomatisasi. Selain itu, SOAR bergantung pada integrasi data intelijen ancaman yang akurat dan terkini, jadi jika data tidak lengkap, efektivitas respons otomatis dapat menurun. Selain itu, pengelolaan yang sulit dan kebutuhan sumber daya yang tinggi menghalangi penerapan SOAR secara luas. Meskipun SOAR membantu mempercepat respons dan mengurangi beban kerja manual, jurnal ini menekankan bahwa pengembangan lebih lanjut diperlukan agar SOAR menjadi lebih fleksibel, efektif, dan mampu menghadapi serangan siber generasi terbaru yang semakin kompleks dan *multi-vektor*.
[10] ARCHITECTURE-CENTRIC SUPPORT FOR SECURITY ORCHESTRATION AND AUTOMATION	Meskipun teknologi SOAR menawarkan banyak otomatisasi dan orkestrasi respons insiden, jurnal "Architecture-Centric Support for Security Orchestration and Automation" mengungkap beberapa kelemahan utama implementasi SOAR. Salah satu masalah utama adalah kesulitan mengintegrasikan berbagai alat keamanan yang berbeda dalam satu *platform* SOAR untuk berhasil, desain arsitekturnya harus fleksibel dan modular. Selain itu, mengelola sistem SOAR seringkali memerlukan keahlian teknis yang kuat, sehingga organisasi dimana kekurangan memiliki sumber daya manusia dan tidak berpengalaman dapat mengalami kesulitan dalam menjalankan dan memelihara sistem ini secara optimal. SOAR juga tidak dapat menyesuaikan diri dengan serangan siber yang sangat dinamis dan kompleks, yang dapat mengurangi efektivitas respons otomatis jika data intelijen ancaman tidak lengkap atau *up-to-date*. Jurnal ini juga menekankan bahwa meskipun SOAR meningkatkan efisiensi dan kecepatan respons insiden, pengawasan manusia diperlukan untuk membuat keputusan yang tepat, sehingga otomatisasi tidak sepenuhnya menggantikan peran analis keamanan. Untuk mengatasi masalah ini, diperlukan pengembangan lebih lanjut dalam hal interoperabilitas, kemudahan penggunaan, dan kecerdasan adaptif.

3.3 Perbandingan implementasi SIEM dan SOAR serta Tantangan di Indonesia

Berikut perbandingan implementasi SIEM dan SOAR yang disajikan dalam table 3 :

Tabel 3. Perbandingan SIEM dan SOAR

SIEM vs SOAR	
Jenis Sumber Data	SIEM mengumpulkan data mentah dari berbagai sumber di seluruh infrastruktur seperti *log* dari *firewall*, *server*, perangkat jaringan, dan aplikasi yang memberikan gambaran *holistik* tentang keamanan suatu organisasi. Sedangkan SOAR dirancang untuk mengotomatiskan proses, sehingga sistemnya perlu memiliki pemahaman yang luas tentang tindakan serta pengaturan jaringan agar mampu mengenali anomaly secara efektif.
Manfaat dan Fungsi	SIEM berfokus pada penyimpanan data, pengumpulan informasi keamanan, serta keperluan analisis. Secara bersamaan, SIEM juga digunakan untuk menggabungkan data, mendeteksi potensi ancaman, melakukan identifikasi, dan memberikan peringatan. Sementara itu SOAR dirancang untuk mengotomatisasikan dan mengatur operasi keamanan data, mengurangi waktu dan upaya yang diperlukan untuk respons insiden, tetapi kinerja SOAR sangat bergantung pada kualitas data yang diperoleh.
Waktu untuk menggunakan	SIEM digunakan ketika ingin memantau dan menganalisis aktivitas keamanan secara *real time*. Misalnya jika ingin memiliki banyak perangkat yang menghasilkan *log*, maka SIEM memiliki kemampuan untuk menganalisis data *log* secara mendetail. SOAR digunakan ketika ingin mempercepat proses respons terhadap insiden keamanan dengan mengotomatisasi berbagai tugas rutin tim keamanan tetapi kinerja SOAR sangat bergantung terhadap kualitas data dan memerlukan integrasi yang cermat agar dapat bekerja optimal

Dikutip dari tabel dan beberapa penelitian tentang kedua implementasi, berikut tantangan implementasi SIEM dan SOAR di Indonesia :

1. Keterbatasan infrastruktur teknologi

   Banyak organisasi di Indonesia masih tidak memiliki infrastruktur TI yang memadai untuk mendukung SIEM dan SOAR secara efektif, terutama di sektor pemerintahan dan bisnis kecil dan menengah.

2. Kekurangan kemampuan SDM

   Ada kekurangan profesional keamanan siber yang berpengalaman dalam mengelola dan mengoperasikan SIEM dan SOAR. Pelatihan dan pengembangan terus diperlukan.

3. Kendala dalam integrasi dengan sistem yang ada

   Banyak organisasi menggunakan sistem legacy, yang sulit diintegrasikan dengan solusi SIEM dan SOAR kontemporer. Akibatnya, proses integrasi menjadi sulit dan memakan waktu.

4. Keterbatasan anggaran dan prioritas keamanan siber

   Ada keterbatasan anggaran keamanan siber dan kurangnya pemahaman manajemen tentang pentingnya investasi dalam SIEM dan SOAR. Kedua faktor ini menghambat adopsi teknologi ini secara luas.

5. Regulasi dan Kepatuhan yang Beragam

Ada banyak regulasi keamanan data yang berbeda di Indonesia, yang memerlukan penyesuaian sistem yang dapat membuat implementasi lebih sulit, terutama bagi organisasi yang harus mematuhi peraturan lokal dan internasional.

6. Kualitas Data dan False Positives

   Data yang tidak lengkap atau tidak konsisten sering menyebabkan false positives, yang membebani tim keamanan di Indonesia.

7. Budaya keamanan organisasi dan kesadaran keamanan

   Beberapa organisasi tidak memiliki budaya dan kesadaran tentang keamanan siber, yang menghambat penggunaan SIEM dan SOAR. Ini karena proses keamanan yang efektif membutuhkan kerja sama lintas fungsi.

4. Kesimpulan

SIEM (Security Information and Event Management) dan SOAR (Security Orchestration, Automation, and Response) adalah dua komponen penting dalam strategi keamanan siber modern. Dalam menghadapi ancaman yang semakin kompleks, keduanya bekerja sama. SIEM berfungsi sebagai pusat analitik yang mengumpulkan dan mengkorelasikan data *log* secara *real-time* dari berbagai perangkat, aplikasi, dan sistem. Kemampuan korelasi data yang kuat dan dukungan untuk berbagai format *log* memungkinkan SIEM memungkinkan organisasi menghasilkan laporan kepatuhan yang menyeluruh serta mendeteksi pola serangan, anomali, dan pelanggaran lebih awal. SIEM berfungsi sebagai komponen penting dari sistem pemantauan keamanan perusahaan karena kemampuan ini.

Sebaliknya, dengan memanfaatkan *playbook* dan integrasi antar sistem keamanan, SOAR berkonsentrasi pada otomasi respons insiden. Efektivitas SOAR sangat bergantung pada data yang dihasilkan oleh sistem seperti SIEM. Jika data yang dimasukkan tidak akurat atau tidak lengkap, proses otomatisasi dalam SOAR berisiko mengeksekusi dengan salah atau tidak mencapai hasil maksimalnya. Dalam artikel ini, ditekankan bahwa penerapan SIEM cenderung memberikan dampak yang lebih signifikan dan permanen terhadap posisi keamanan organisasi, terutama dalam hal visibilitas, deteksi dini, dan kepatuhan terhadap peraturan.

Oleh karena itu, meskipun SOAR menawarkan banyak manfaat dalam hal efisiensi operasional, keberhasilan implementasi SIEM sangat bergantung pada ekosistem yang dibangunnya. Sehingga, organisasi disarankan untuk memprioritaskan implementasi SIEM yang matang sebelum melanjutkan ke tahap otomatisasi dengan SOAR. SIEM bukan hanya menyediakan fondasi data tetapi juga memberikan konteks yang sangat dibutuhkan agar respons yang dihasilkan melalui SOAR benar-benar relevan. Oleh karena itu, SIEM layak dianggap sebagai investasi penting secara strategis dalam membangun sistem keamanan siber yang kuat dan berkelanjutan.

Sebagai pandangan pribadi penulis, Masa depan pengembangan SIEM dan SOAR akan mengarah pada integrasi yang lebih cerdas dan otomatis, terutama dengan dukungan AI dan ML. Dengan segala kemungkinan, SIEM akan berfungsi sebagai alat pelaporan dan deteksi serta penyedia data kontekstual yang mendukung respons otomatis SOAR. Namun, masalah seperti kekurangan sumber daya manusia, kesiapan infrastruktur TI, dan kurangnya integrasi sistem masih menjadi hambatan besar untuk implementasi di Indonesia. Akibatnya, penulis percaya bahwa mengambil langkah-langkah bertahap untuk mematangkan implementasi SIEM terlebih dahulu adalah tindakan strategis yang tepat. Ini akan memungkinkan adopsi SOAR di masa mendatang lebih efisien dan sesuai dengan kebutuhan lokal organisasi.

Daftar Pustaka

Alfiansyah, F., & Murad, Skom., Mkom, F. A. (2020). Implementasi Security Information and Event Management (SIEM) pada lingkungan ITSEC Asia menggunakan Elastic SIEM.

Alhakami, W. (2024). Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS, 1–25.

Anggara, T. R. (2023). Strategi implementasi SIEM untuk mengurangi risiko terhadap kebocoran informasi. *Jurnal Teknologi Terpadu.*

Anisarida, A. A., Hafudiansyah, E., & Kurniawan, E. (2020). Perencanaan tebal perkerasan ruas jalan a di Kabupaten Lebak. *Jurnal Teknik Sipil Cendekia (JTSC), 1*(1), 1–14. https://doi.org/10.51988/vol1no1bulanjulitahun2020.v1i1.4

A. Setiyadi, & E. B. Setiawan. (2018). Information system monitoring access log database on database server. *IOP Conference Series: Materials Science and Engineering.*

Ehis, A.-M. T. (2023). Optimization of Security Information and Event Management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture. *Archive of Advanced Engineering Sains*, 1–10.

Gustina, V., & Ananda. (2024). Kecerdasan buatan untuk security orchestration, automation and response: Tinjauan cakupan. *Jurnal Komputer Terapan*, 36–47.

Hafiz, M., & Soewito, B. (2022). Information security systems design using SIEM, SOAR and Honeypot. *Jurnal Pendidikan Tambusai*, 15527–15541.

Harsono. (2022). Faktor-faktor yang mempengaruhi sistem informasi berbasis komputer: Sistem operasi, server, dan programmer (literature review executive support system for business). *Jurnal Manajemen Pendidikan dan Ilmu Sosial.*

Heluka, H. D., & Sulisyto, W. (2023). Perancangan dan implementasi Security Information and Event Management (SIEM) pada layanan virtual server. *Jurnal Ilmiah Komputer*, 912–922.

Issenoro, Trisnawati, H., Tarigan, S. O., Faizah, N. M., & Veranita. (2025). Perancangan dan pengembangan aplikasi deteksi anomali pada jaringan internet gedung Disaster Recovery Center Badan Diklat Kejaksaan RI dengan implementasi sistem manajemen informasi dan keamanan (SIEM) berbasis web. *Jurnal Ilmu Komputer dan Teknologi Informasi.*

Islam, C. (2020). Architecture-centric support for security orchestration and automation.

Lintasarta. (2020, Desember 11). Perbedaan SIEM dan SOAR dalam keamanan siber. https://www.lintasarta.net/blog/solution/it-services/security-it-services/perbedaan-siem-dan-soar-dalam-keamanan-siber/

Paw, M. P., Aspriyono, H., & Al Akbar, A. (2024). Implementasi Security Information dan Event Management (SIEM) dalam melakukan monitoring jaringan pada SMA 1 Muhammadiyah Boarding School. *Jurnal Media Computer Science.*

Rasyidi, B., & Pratama, F. (2024). Sistem monitoring server di PT. XYZ Media Indonesia berbasis Grafana dan Prometheus. *Indonesian Journal of Machine Learning and Computer Science*, 1456–1465.

Rizkilina, T. M., & Rosyid, N. R. (2022). Rancangan sistem otomatisasi packet filtering berdasar sinkronisasi data pada IP Profile Database menggunakan Python. *Journal of Internet and Software Engineering (JISE).*

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020). Log event management server menggunakan Elastic Search Logstash Kibana (ELK Stack). *Jurnal Teknologi Informasi dan Multimedia*, 12–20.

Wahid, A., Agung, M., Parenreng, J., Amin, F. H., & Luhriyanti, S. (2024). PKM pengembangan sistem monitoring keamanan server aplikasi SIMLP2M UNM menggunakan Wazuh. *Jurnal VOKATEK*, *2*.